

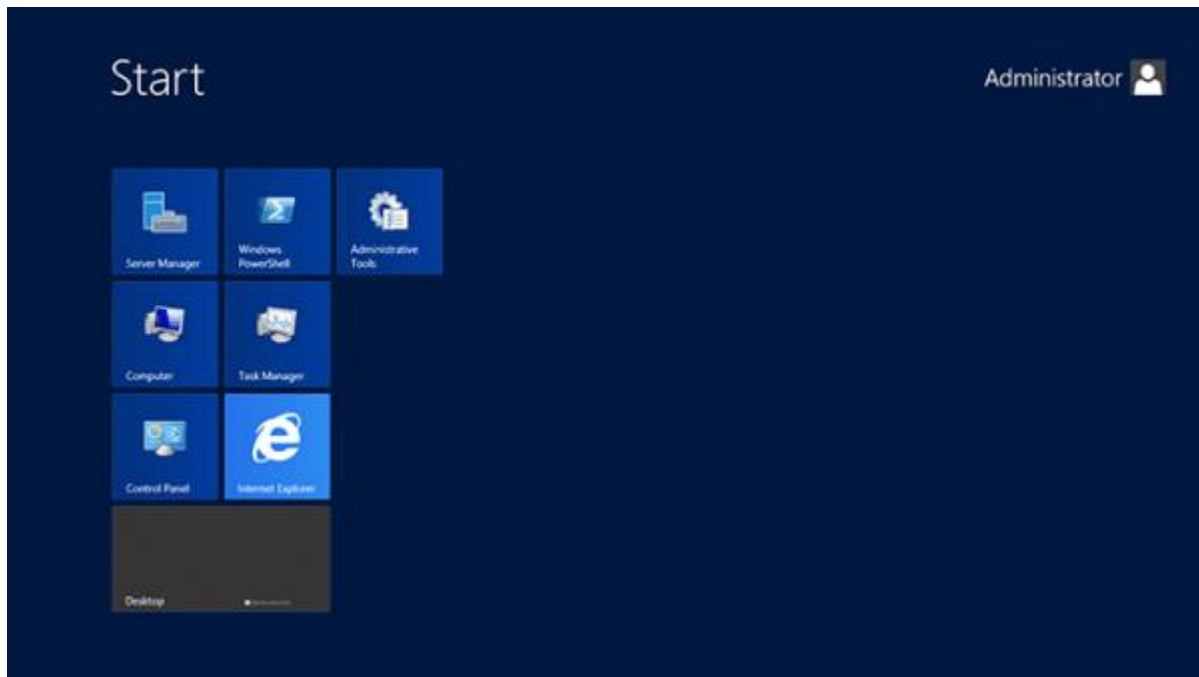
Các bước tiến hành:

- 1. Cài đặt Windows Server 2012**
- 2. Nâng cấp Domain Controller trong Windows Server 2012 R2**
- 3. Tạo Users, OU và phân quyền quản lý OU trên Windows Server 2012**

1. Cài đặt Windows Server 2012

Windows Server 2012 là một hệ điều hành dành riêng cho máy chủ. Để cài Windows Server lên máy ảo VMWare cần phiên bản VMWare từ 9.0 trở lên.

Download Windows Server 2012 R2 Full



Các bước:

Cài đặt Windows Server 2012;
Đặt lại tên (Computer Name) và khai báo địa chỉ IP cho máy chạy Windows Server 2012.

Chuẩn bị:

- Đĩa CD cài đặt Windows Server 2012 (hoặc file iso cài đặt Windows Server 2012).
- Chọn chế độ boot từ CDROM cho máy tính cài đặt.

- Password của tài khoản Administrator; Tên và địa chỉ IP của Server.

Cài đặt Winserver 2012:

Bước 1: Đặt đĩa cài đặt vào ổ CD của Server, Reset lại máy nhấn phím bất kỳ để boot đĩa

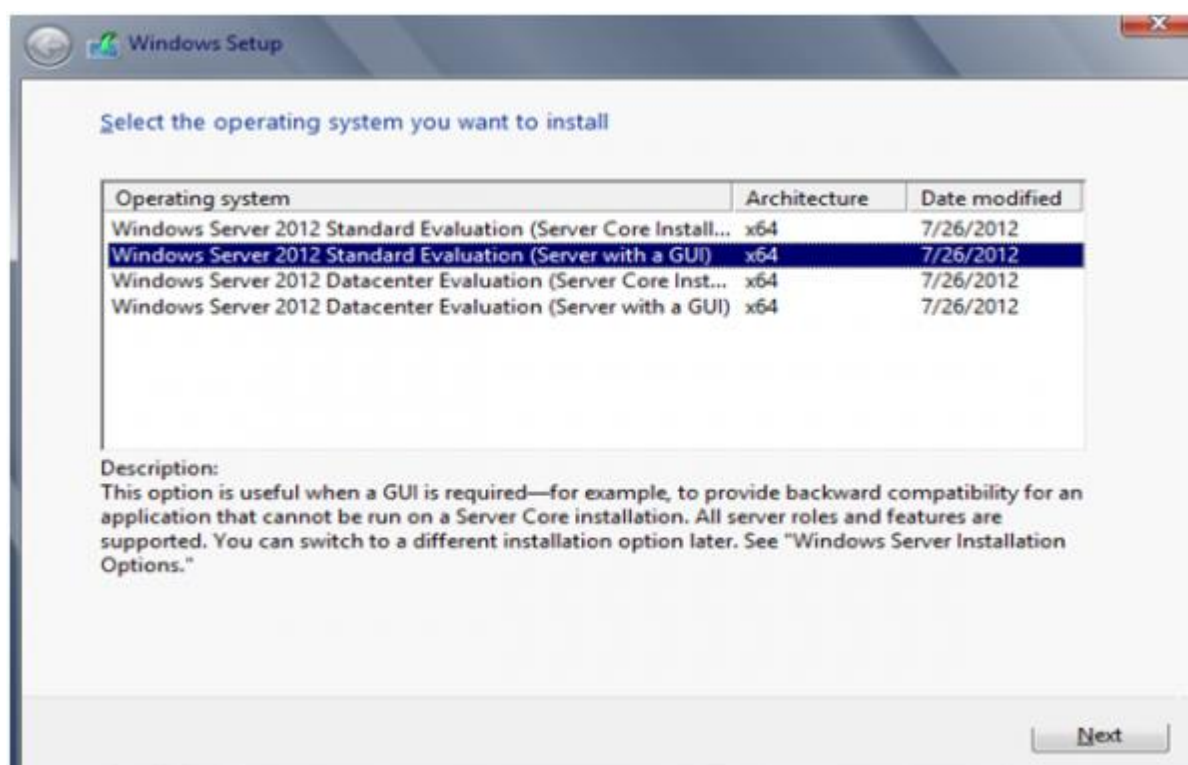
Bước 2: Chọn ngôn ngữ cài đặt rồi nhấn Next



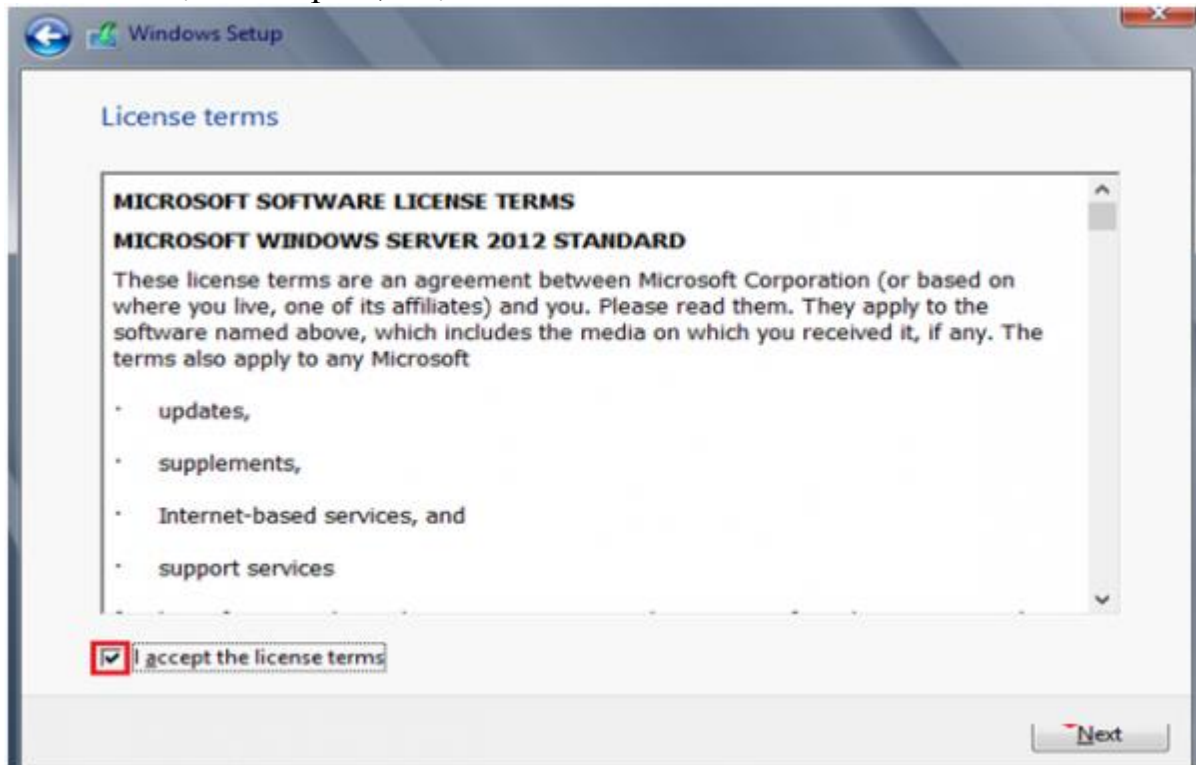
Bước 3: Chọn Install now



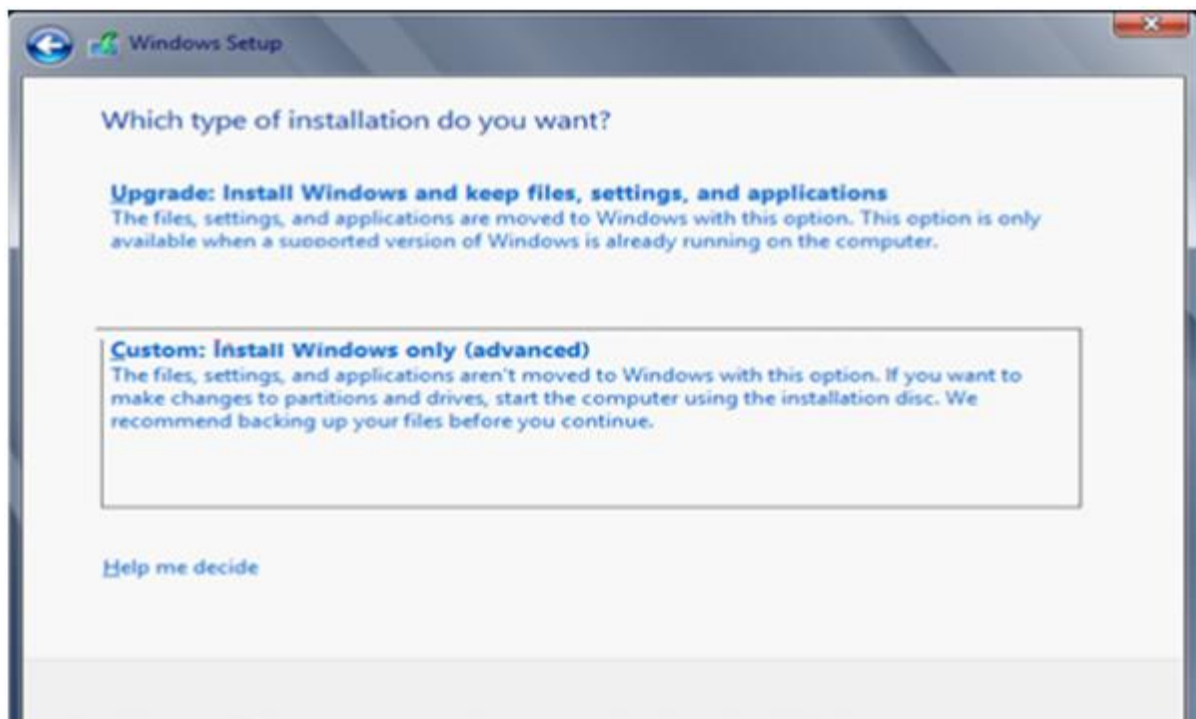
Bước 4: Chọn giao diện đồ họa (GUI)



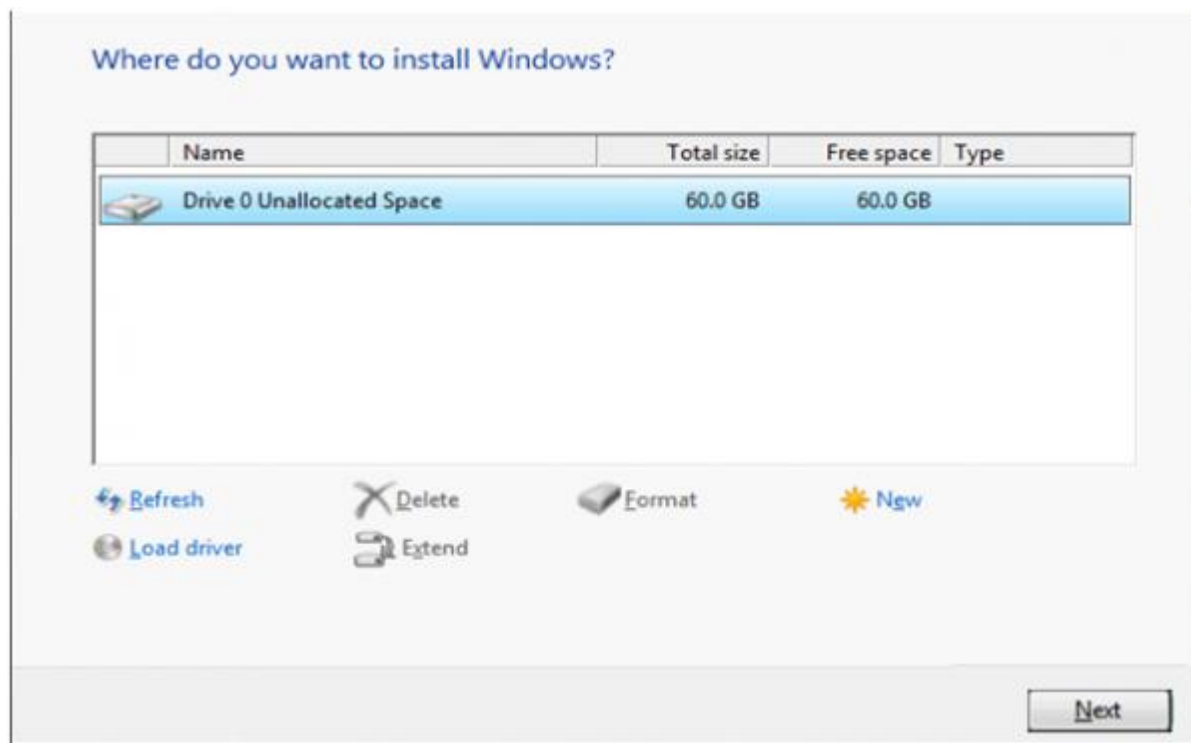
Bước 5: Chọn I accept..., chọn Next



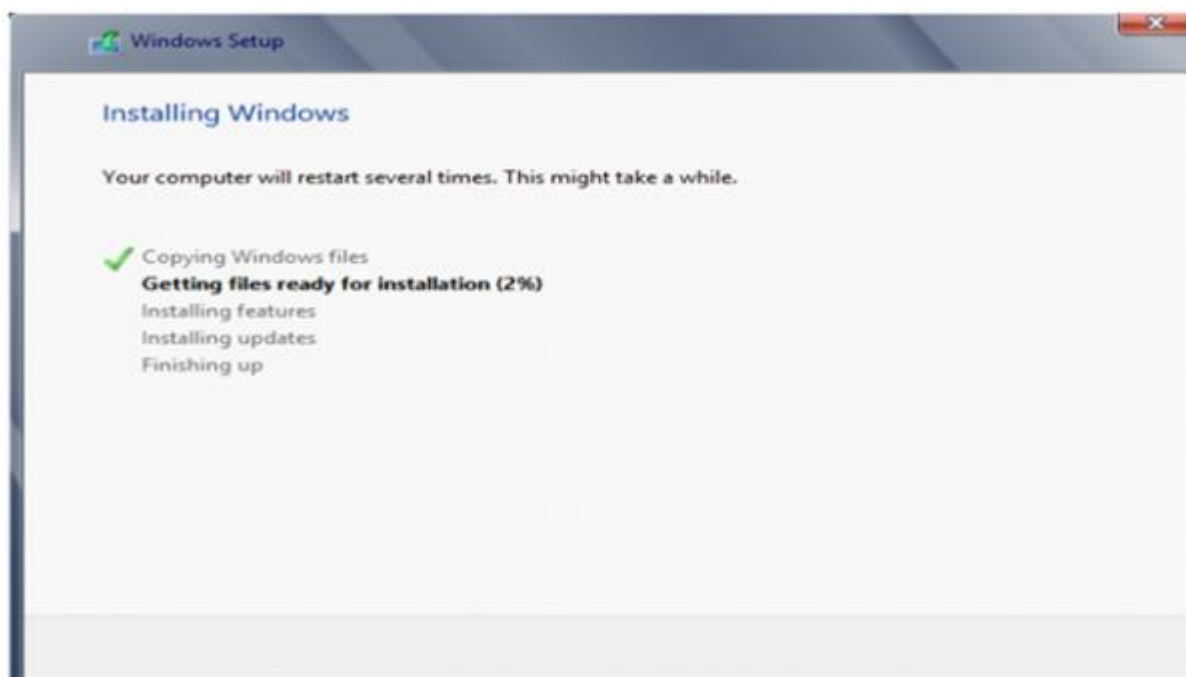
Bước 6: Chọn như hình (Custom....), nhấn Next (tùy chọn khi cài đặt)



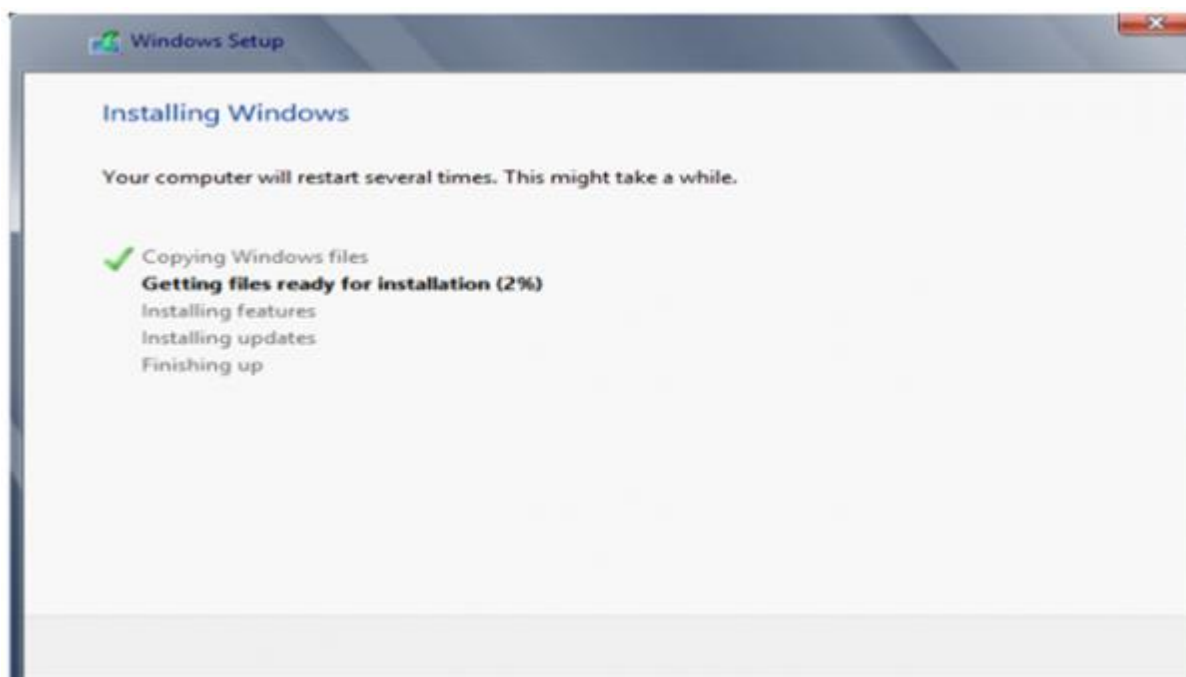
Bước 7: Chọn phân vùng để cài đặt



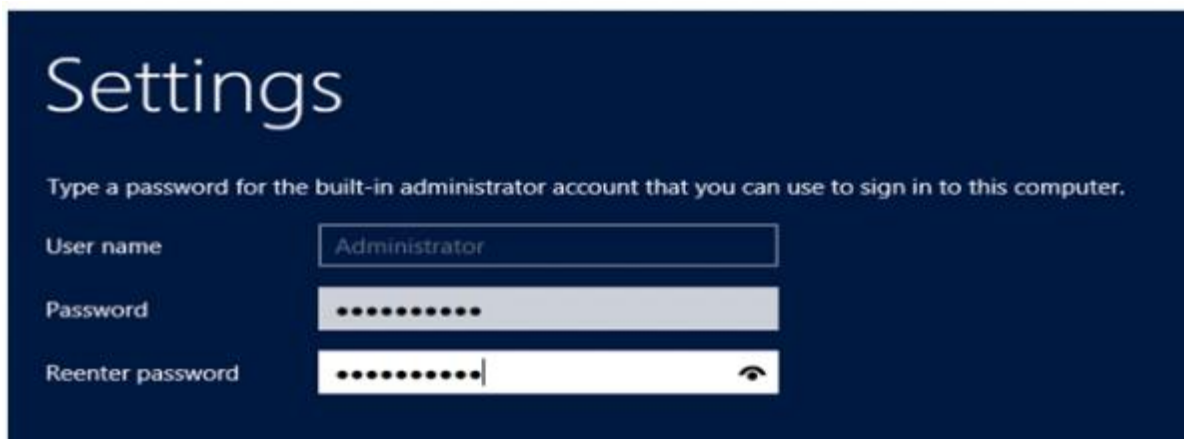
Bước 8: Quá trình cài đặt mất khoảng hơn 20 phút



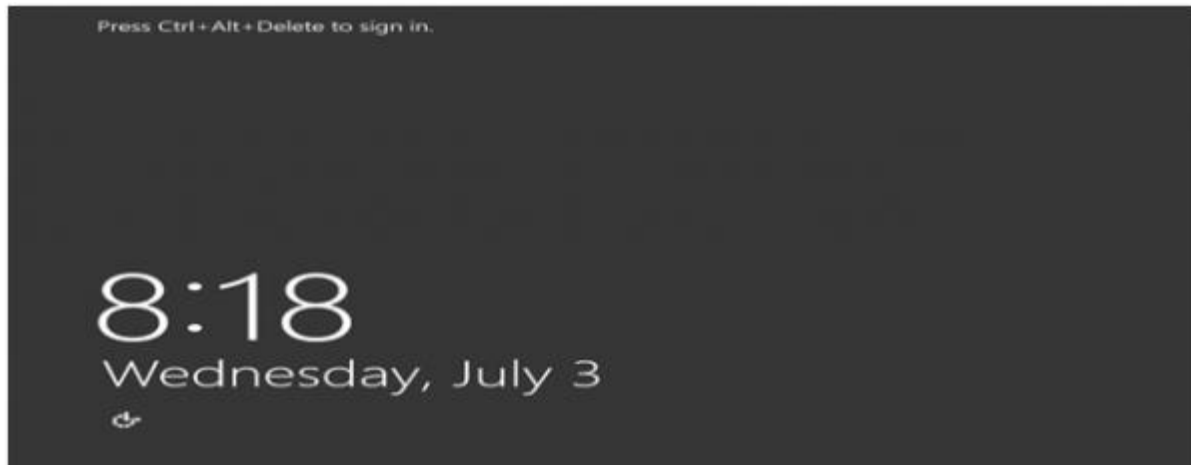
Bước 9: Cài đặt xong máy khởi động lại



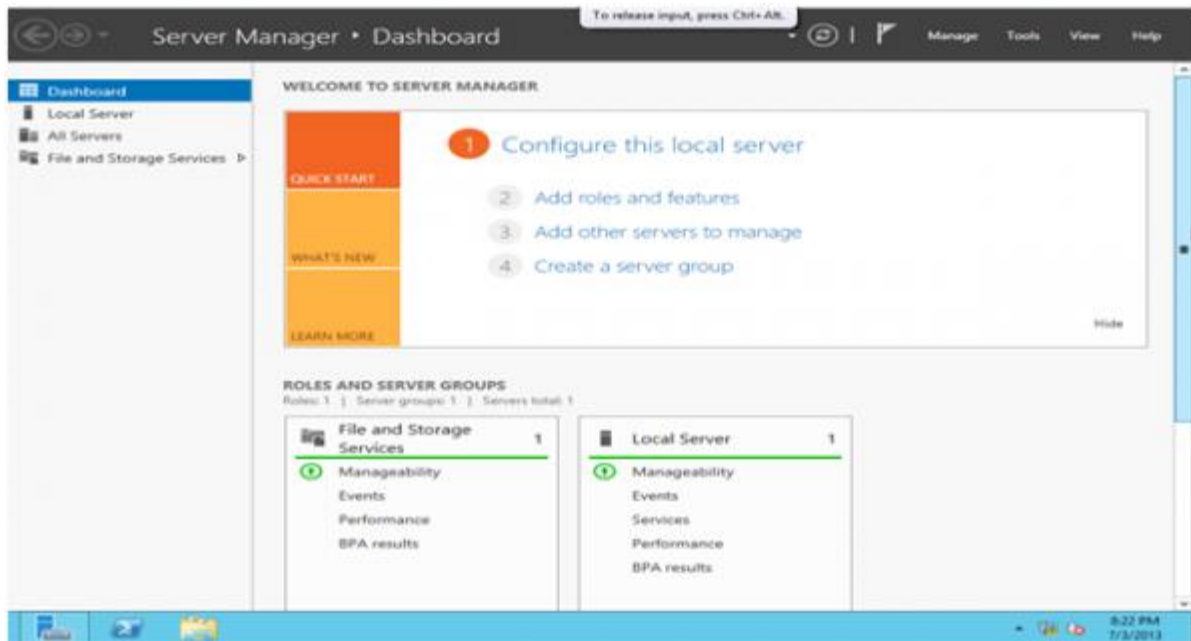
Bước 10: Nhập mật khẩu Administrator: Abc123456



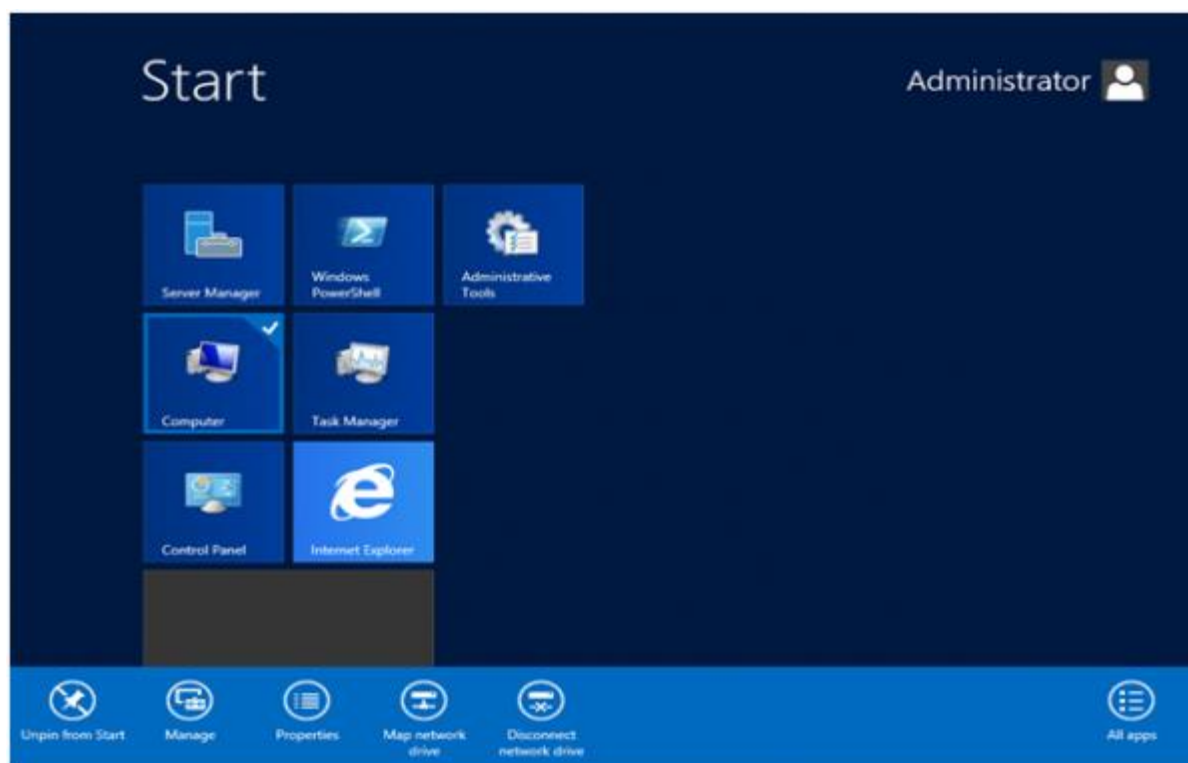
Bước 11: Nhấn Ctrl + Alt + Del để Login



Ngay sau khi cài đặt, giao diện quản lý Server Manager xuất hiện

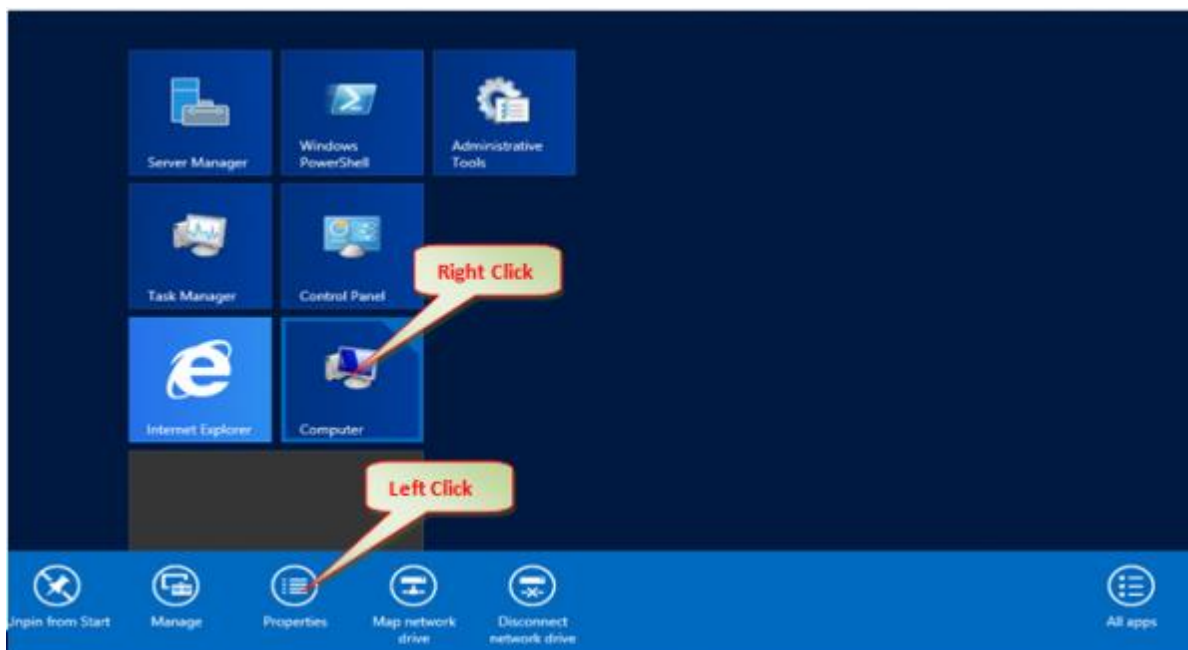


Đây là giao diện Start của Windows Server 2012

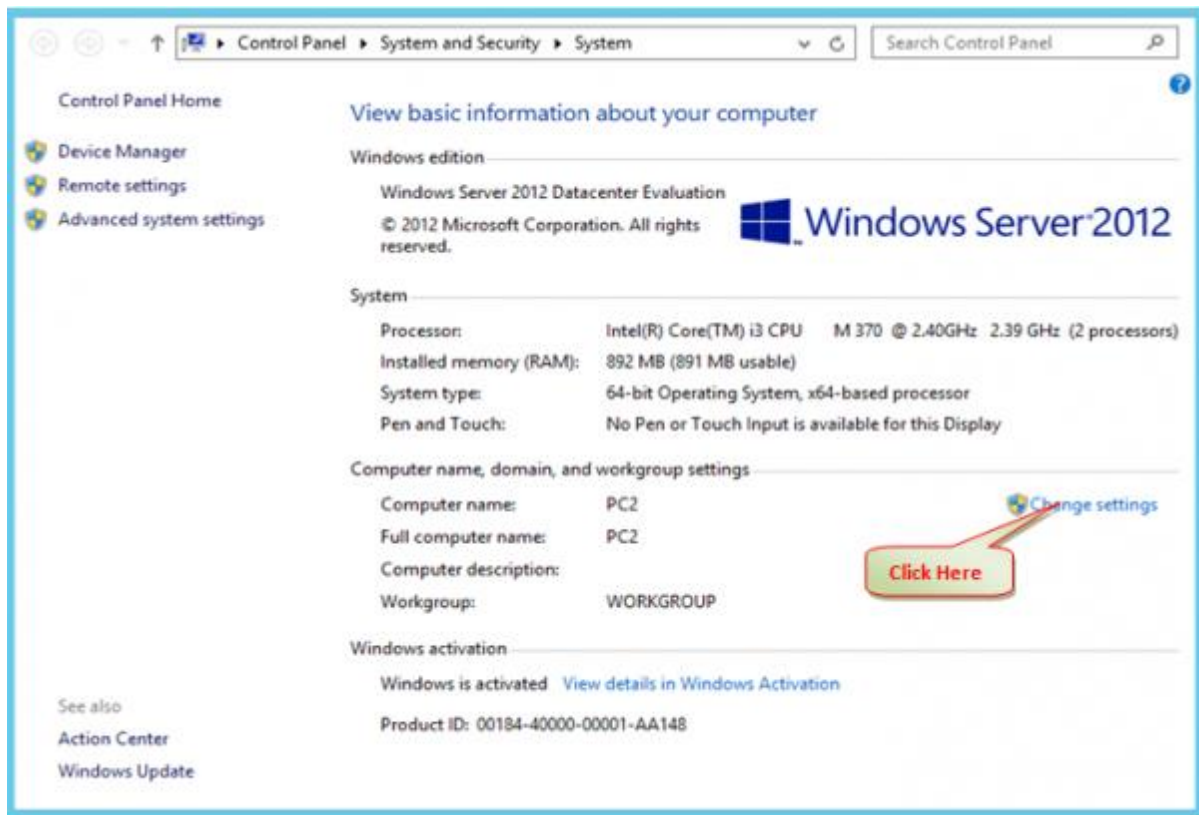


Đặt lại tên máy chạy Winserver 2102:

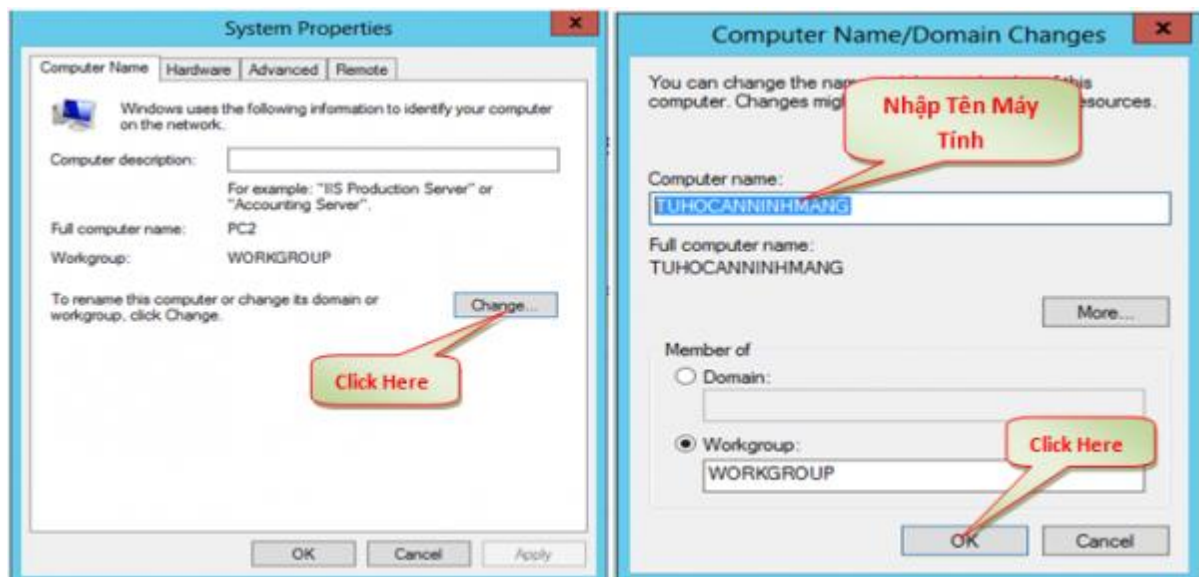
Bước 12: Đổi tên máy tính, Click chuột phải vào Computer chọn Properties



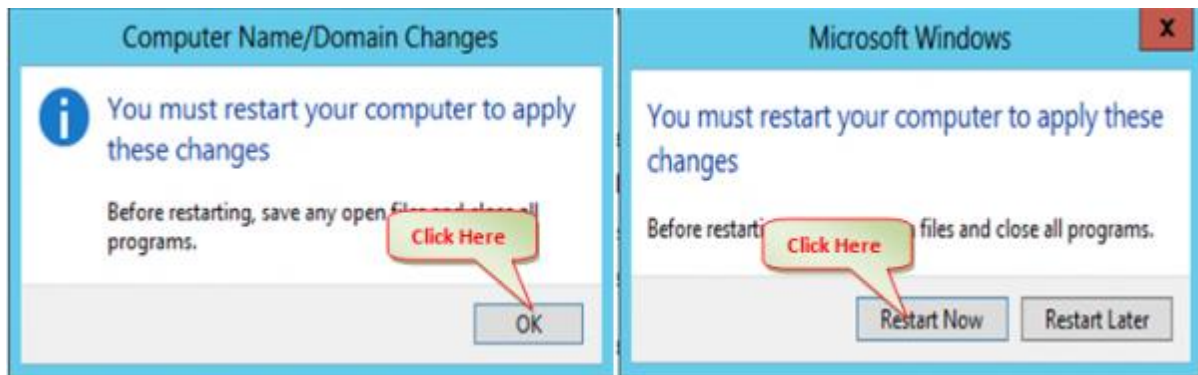
Bước 13: Chọn Change settings



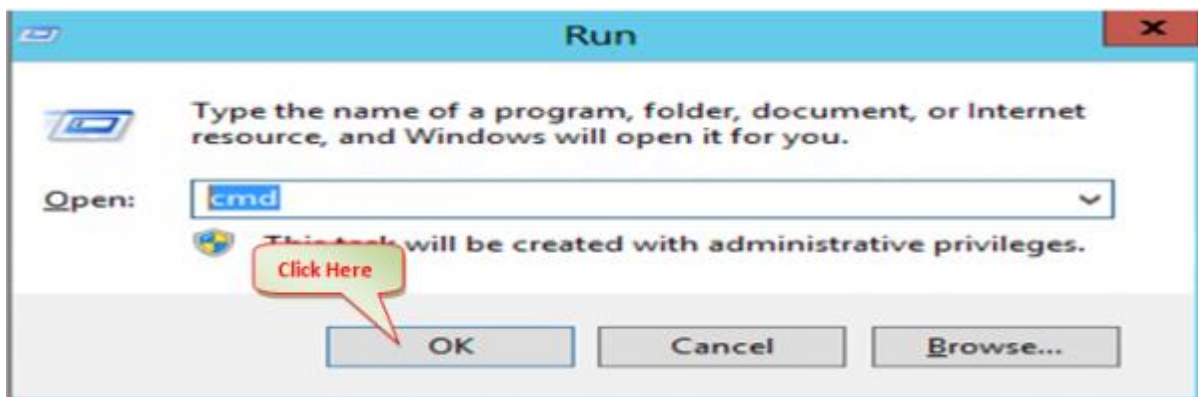
Bước 14: Điền vào tên mới vào hộp Computer Name



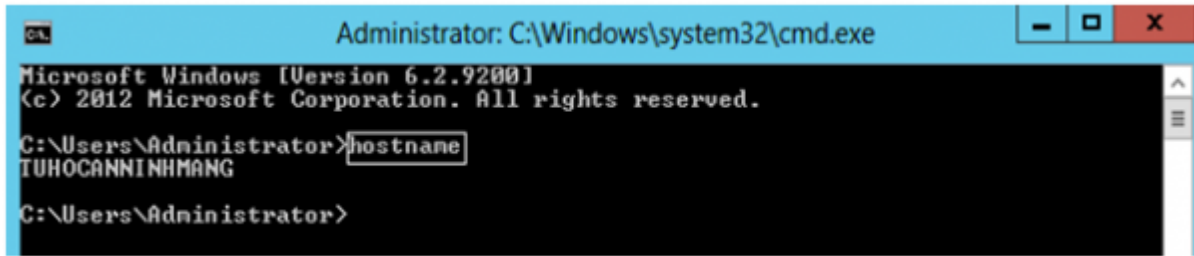
Bước 15: Khởi động lại máy để Apply tên máy



Bước 16: Kiểm tra tên máy sau khi thay đổi bằng cách: Nhấn tổ hợp phím Start + R để mở cửa sổ Run gõ lệnh cmd > OK



Cửa sổ dòng lệnh cmd hiện ra đánh lệnh “hostname” > Enter sẽ thấy được tên máy tính.



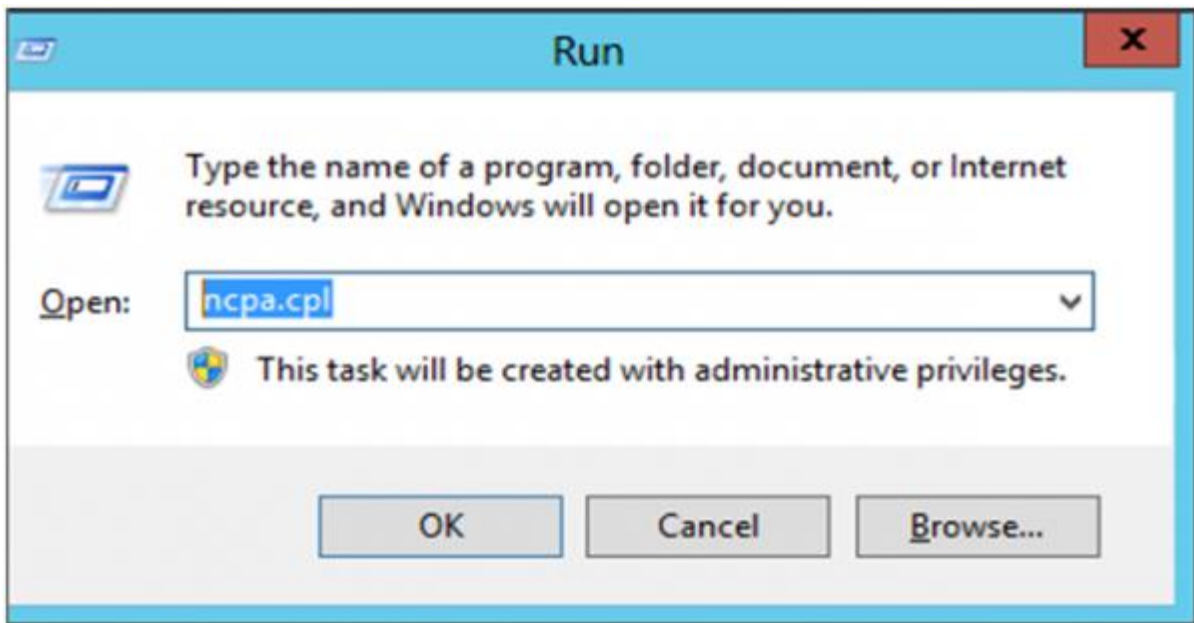
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>hostname
TUHOCANNINHMANH

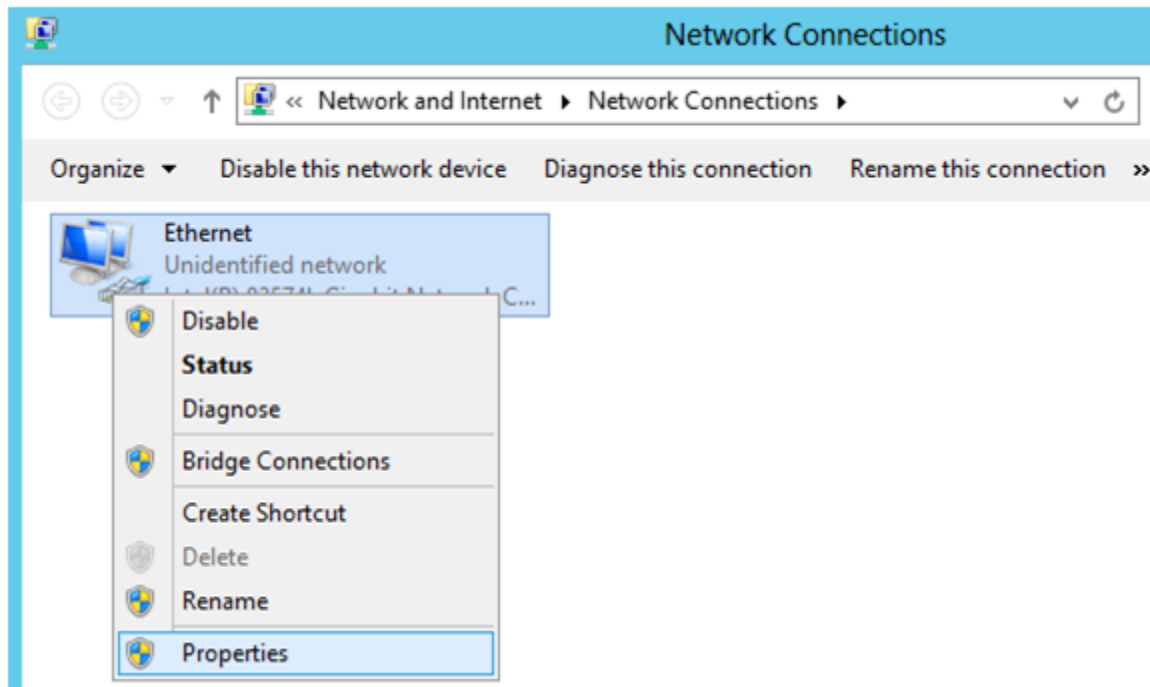
C:\Users\Administrator>
```

Đặt lại địa chỉ cho máy chạy Winserver 2012:

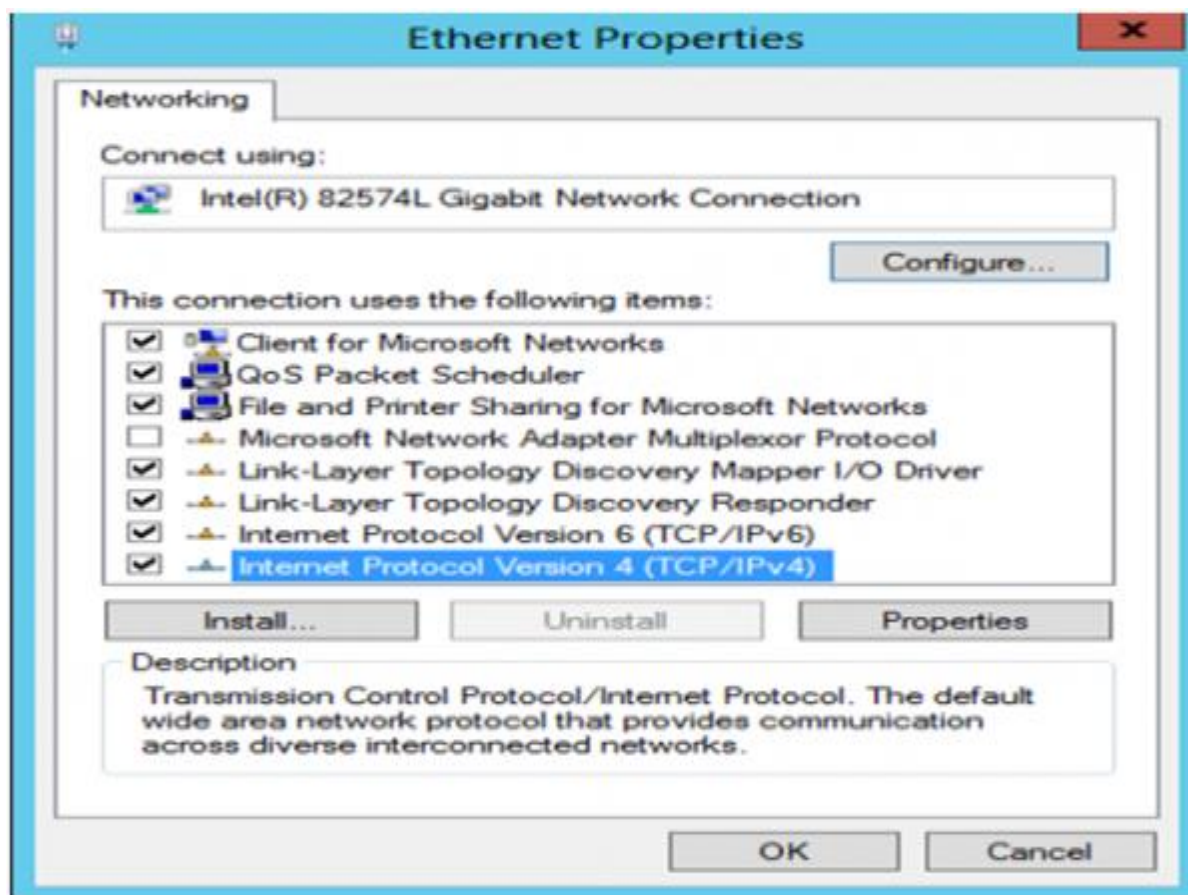
Bước 17: Nhấn tổ hợp phím Start + R mở cửa sổ Run đánh lệnh “ncpa.cpl” > OK



Kích chuột phải vào biểu tượng Card mạng chọn Properties

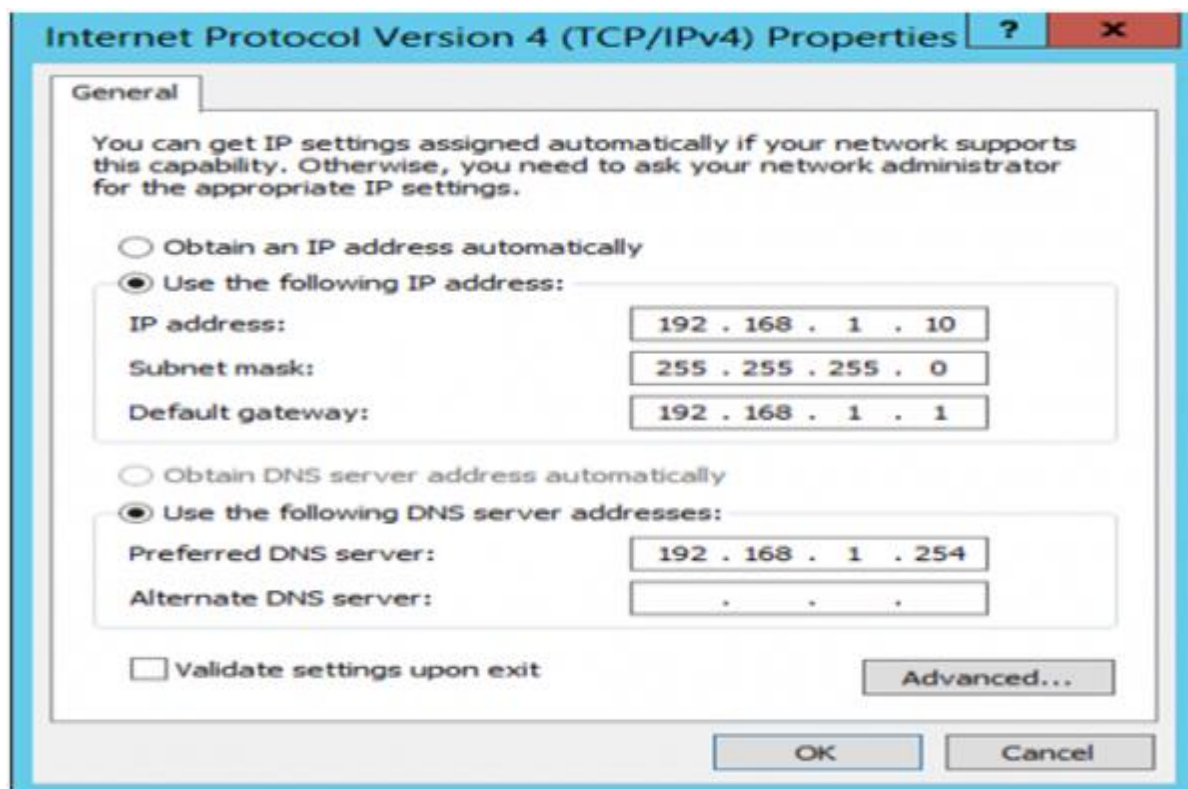


Double Click Internet Protocol Version TCP/IPv4

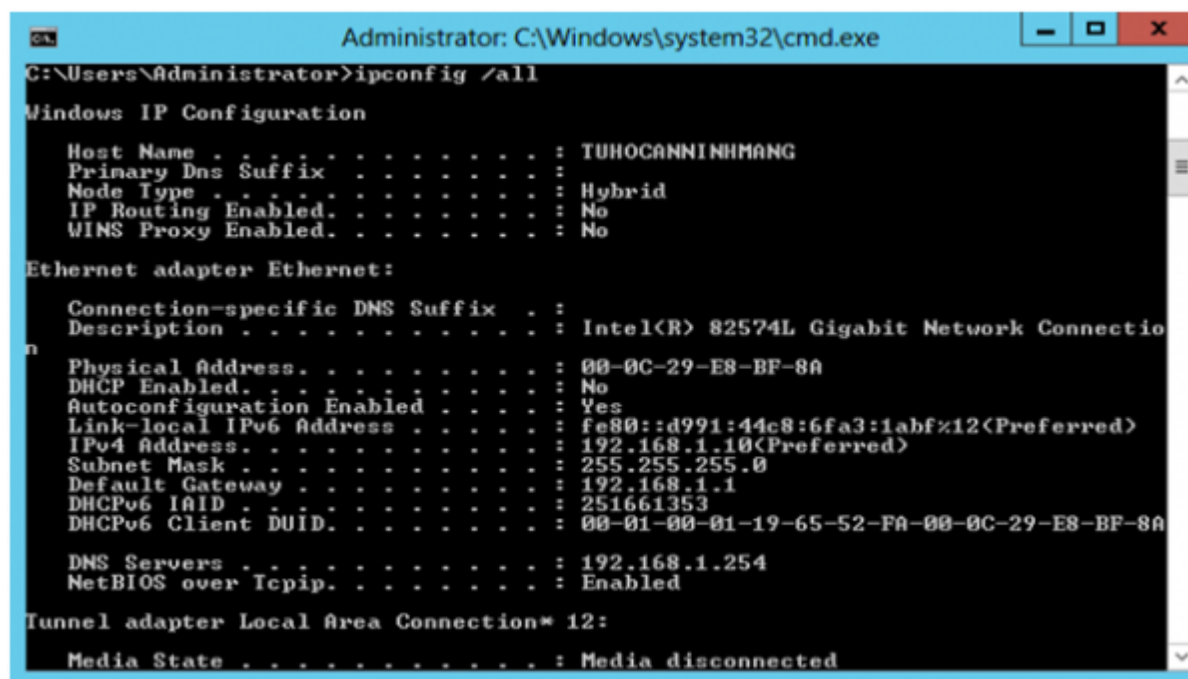


Kích chọn Use the following IP address: Để đặt địa chỉ IP tĩnh cho máy

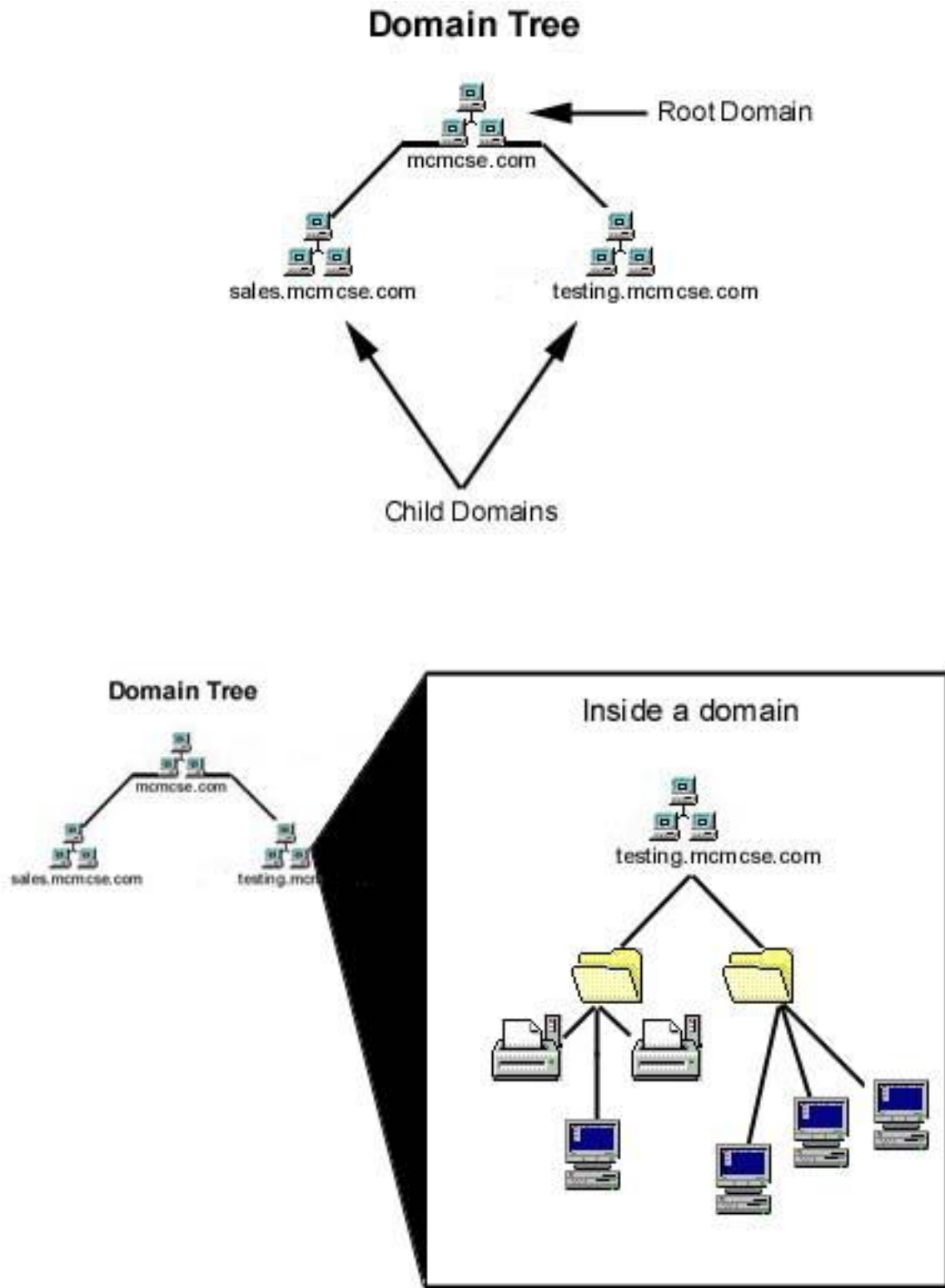
Kích chọn Use the following DNS server addresses: Để đặt địa chỉ DNS server



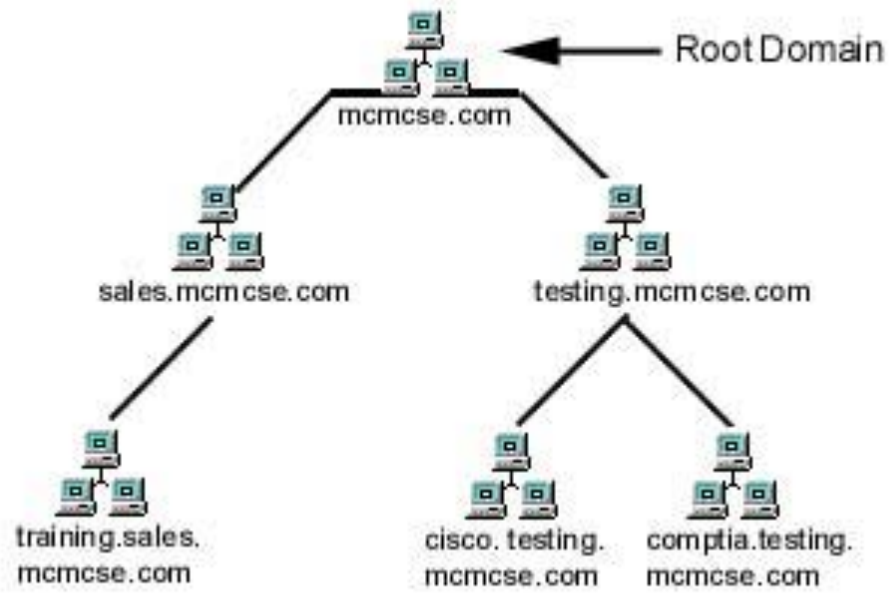
Kiểm tra địa chỉ IP vừa đặt bằng cách: Nhấn tổ hợp phím Start + R, cửa sổ Run gõ lệnh cmd > OK. Trên cửa sổ dòng lệnh cmd gõ lệnh “ipconfig /all”



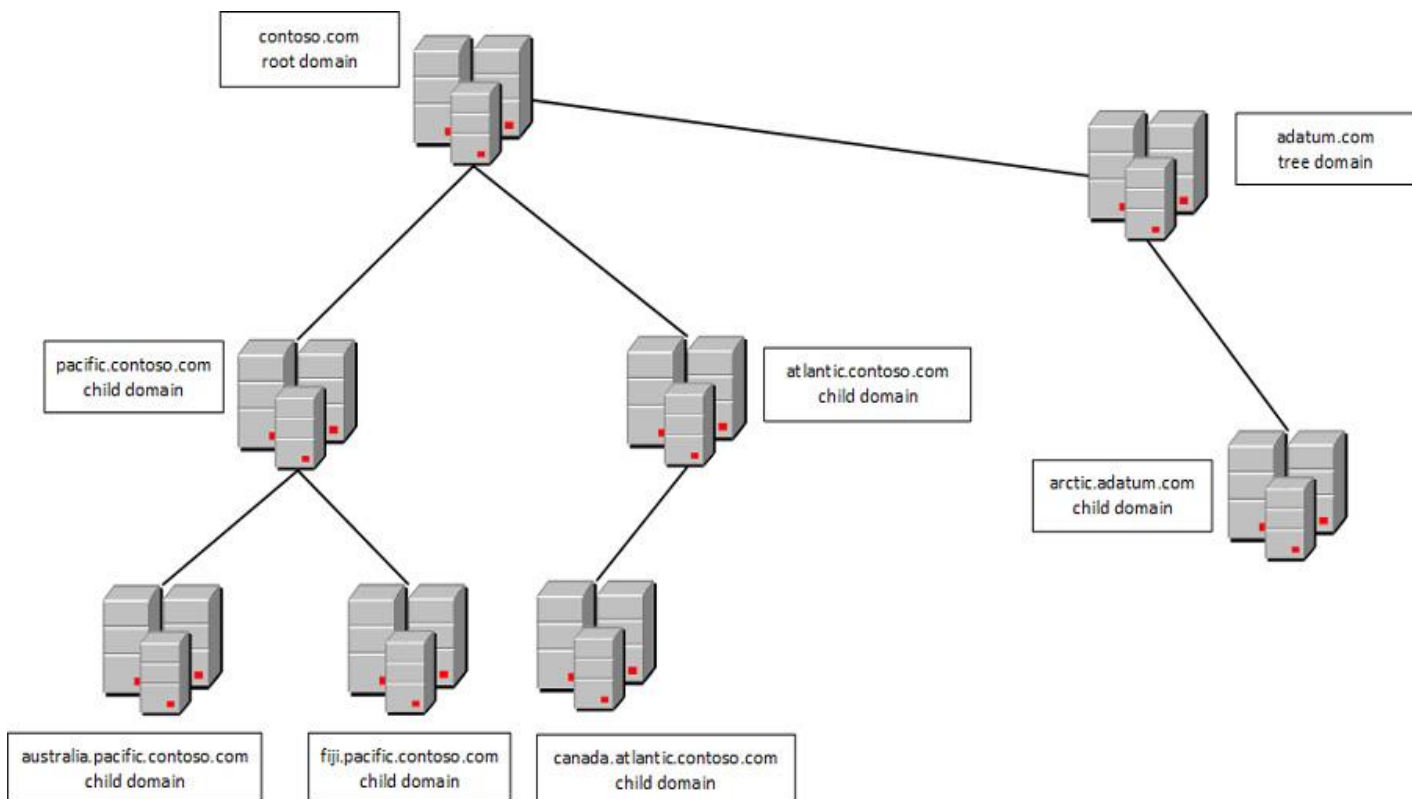
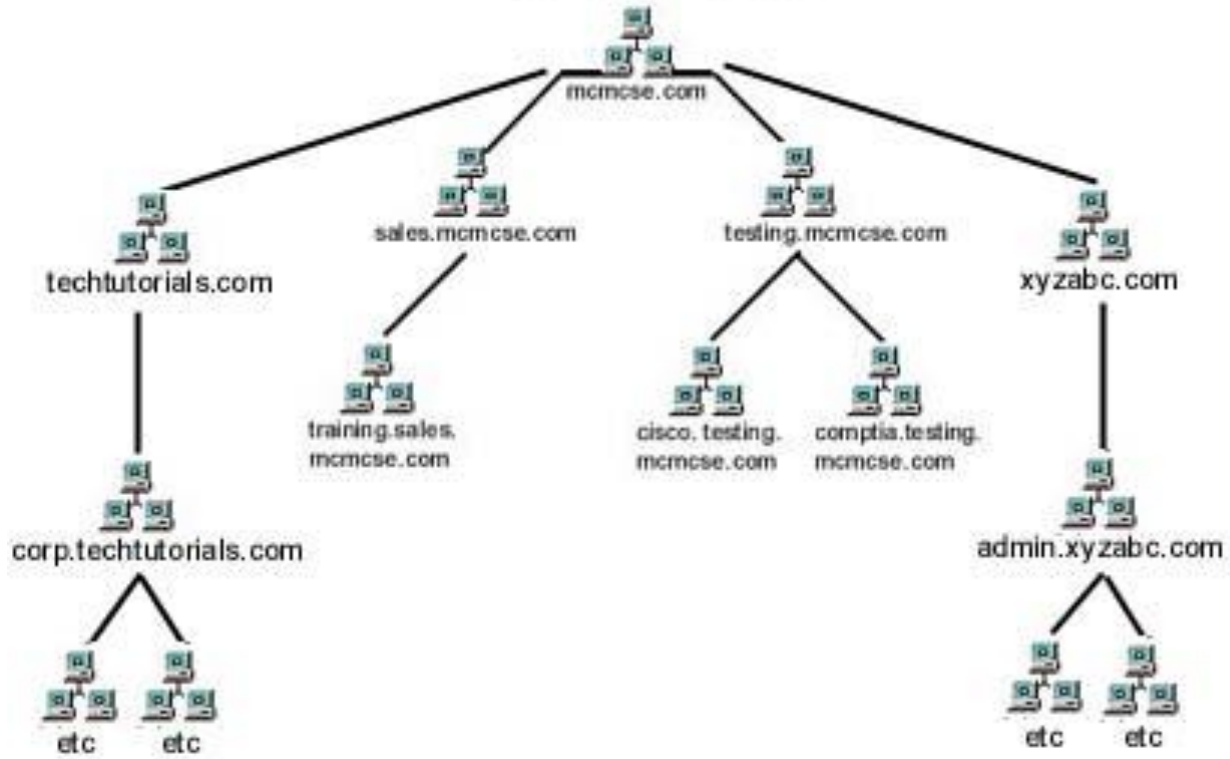
2. Nâng cấp Domain Controller trong Windows Server 2012 R2



Domain Tree



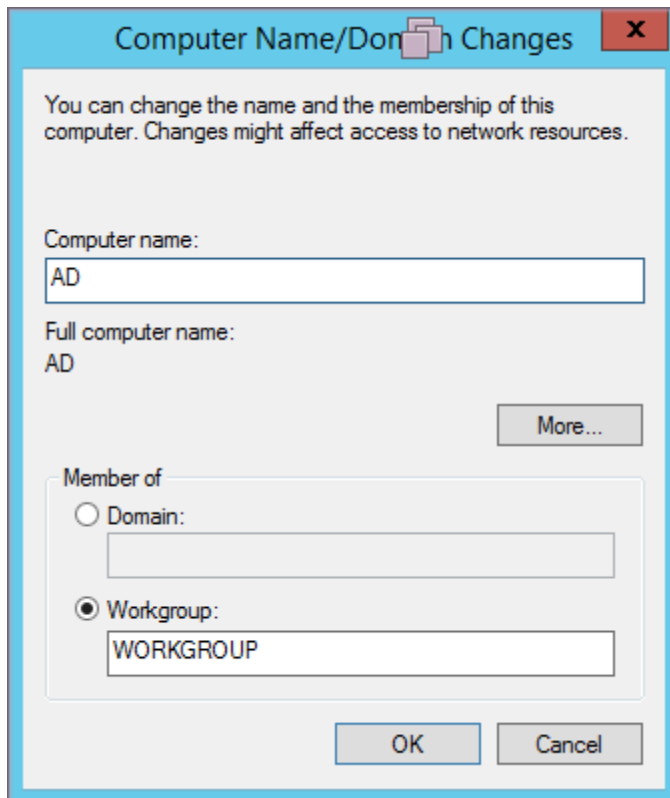
Domain Forest



Sau khi đã cài đặt Windows Server 2012 R2, bước tiếp theo ta nâng cấp máy này thành Domain Controller (DC).

- Forest: mangmaytinh.com
- IP máy DC +DNS : 192.168.1.1/255.255.255.0

1) Change Computer Name của máy



2) Đặt IP kèm DNS trở về máy DC

Internet Protocol Version 4 (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1

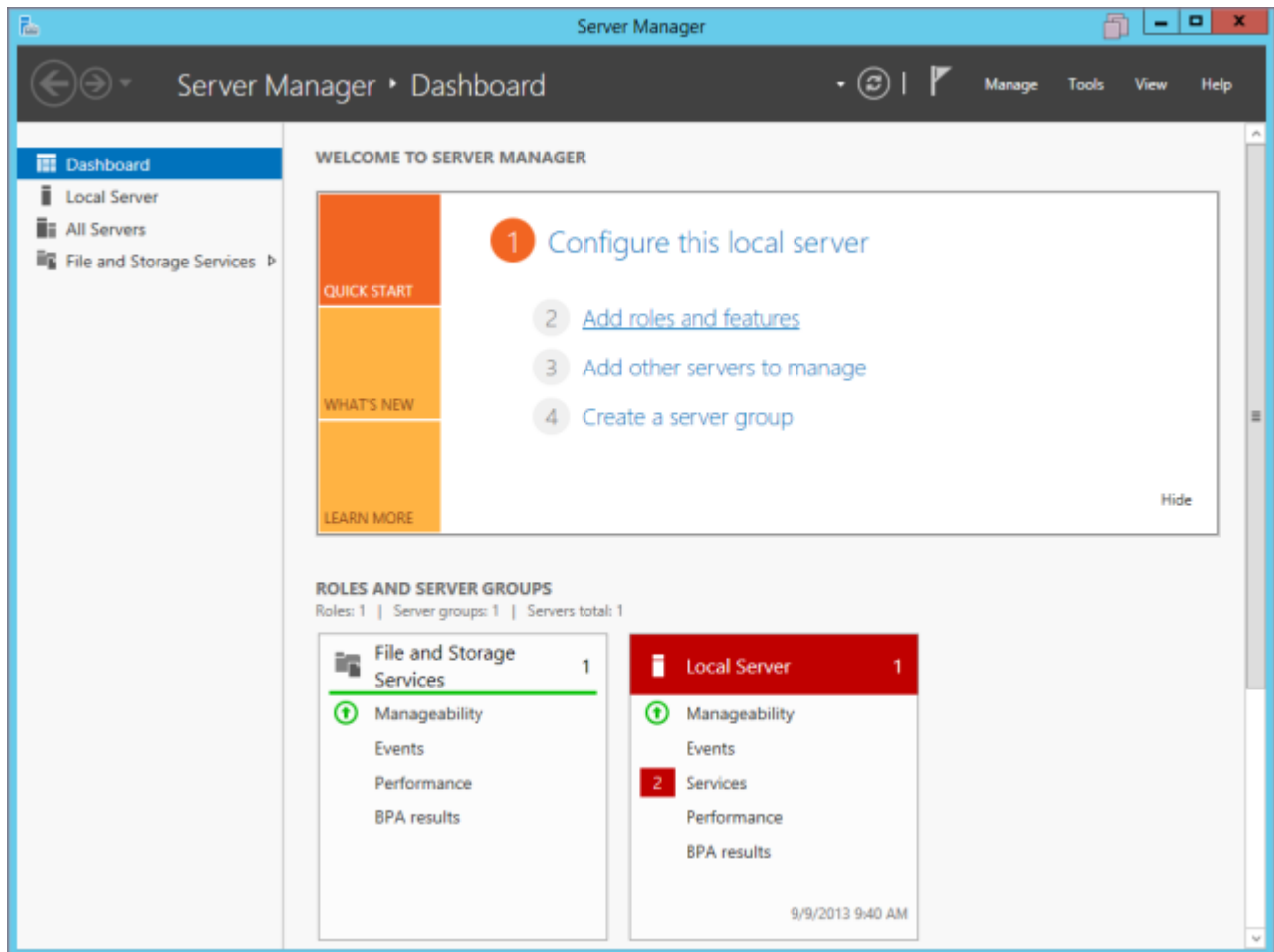
Alternate DNS server: . . .

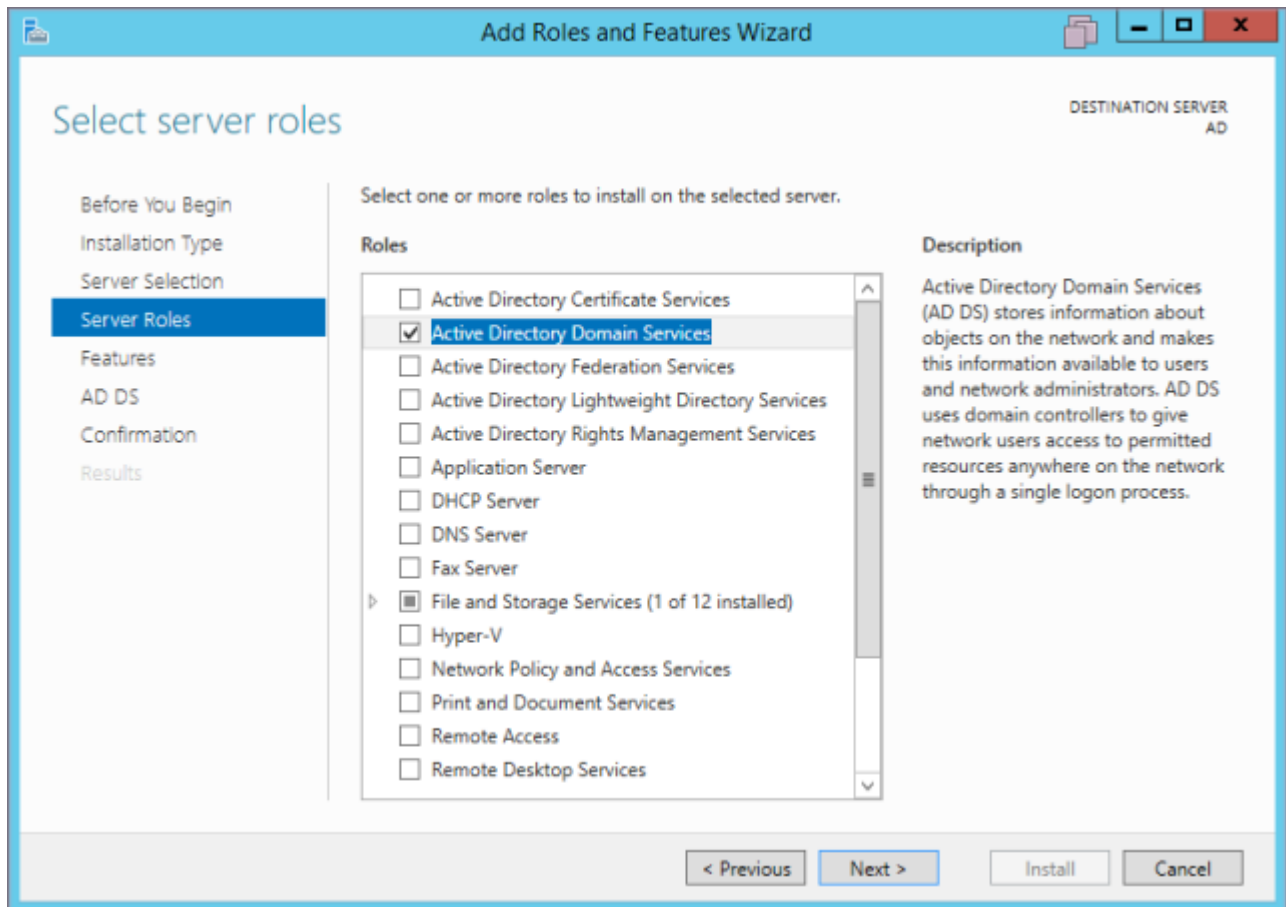
☐ Validate settings upon exit

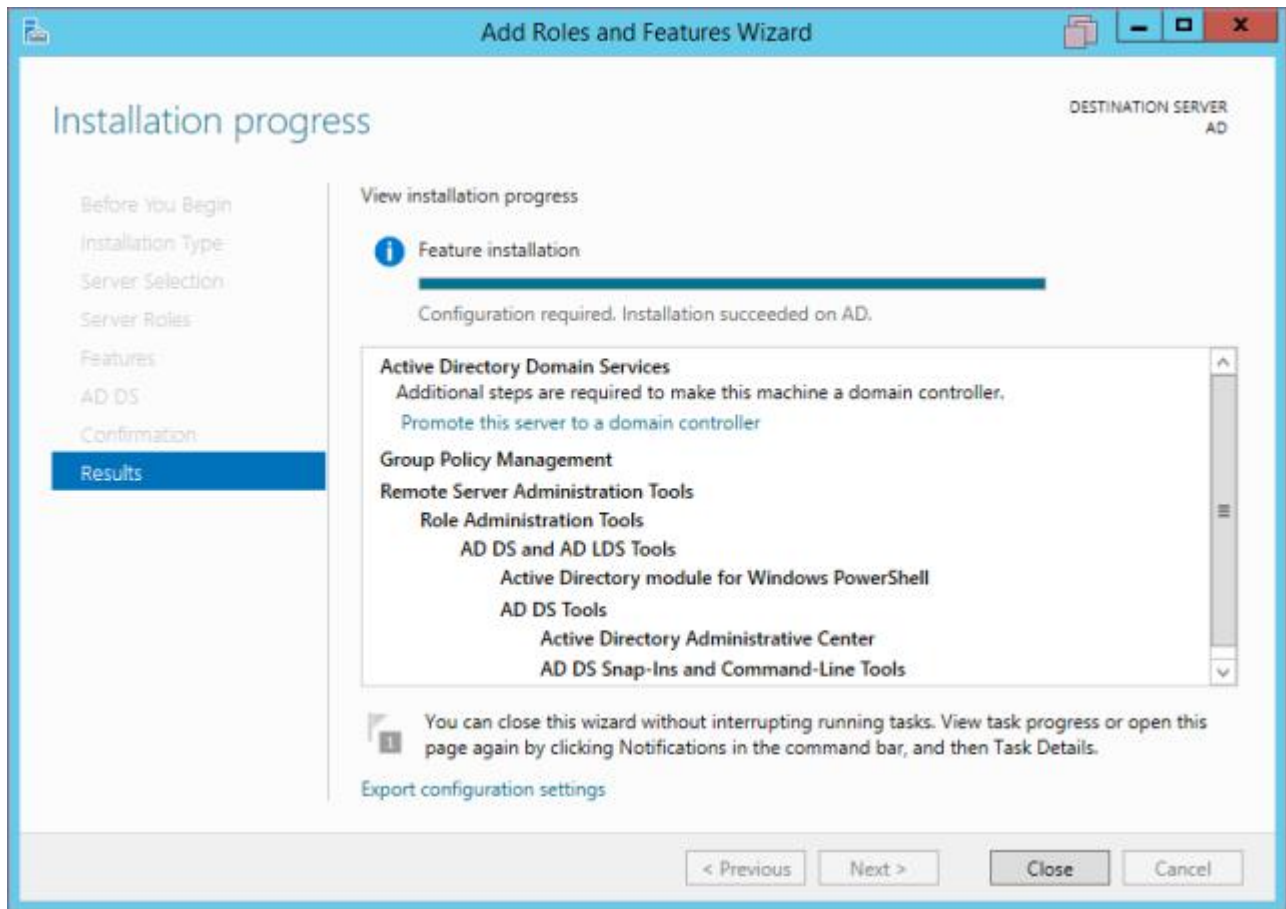
Advanced...

OK Cancel

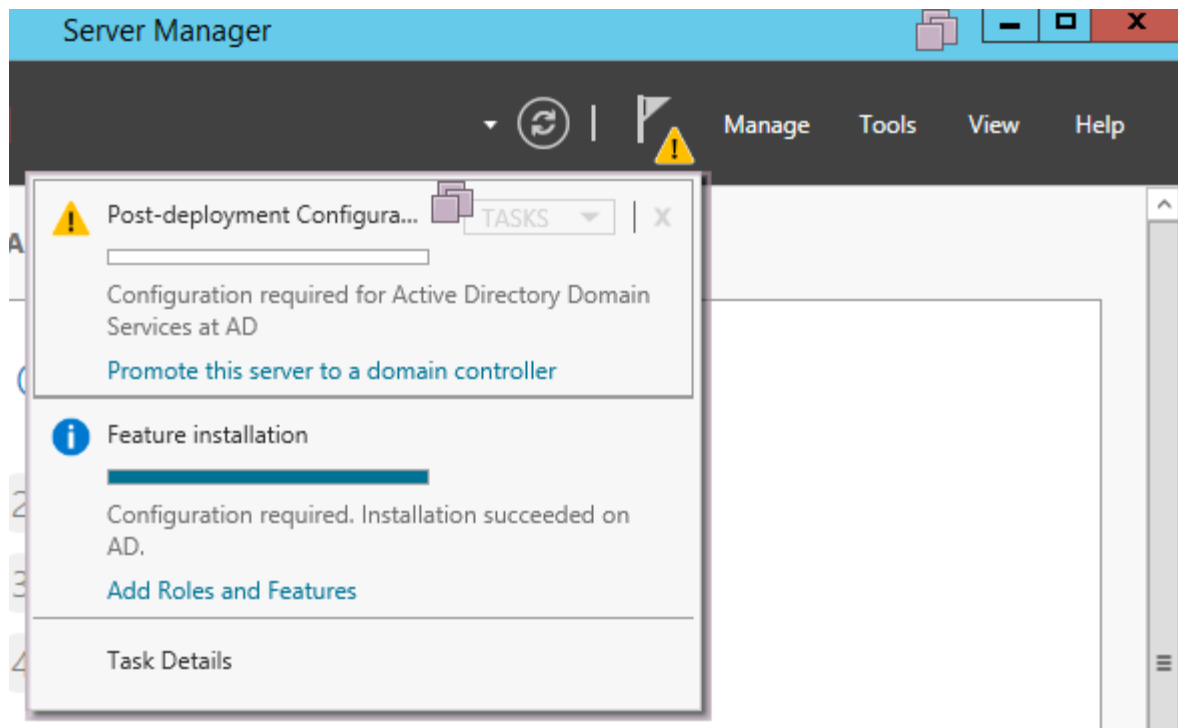
3) Từ Windows Server 2012 đã bỏ cơ chế dcpromo.exe, thay vào đó ta phải cài role “Active Directory Domain Service” mới có thể nâng cấp máy lên thành máy DC



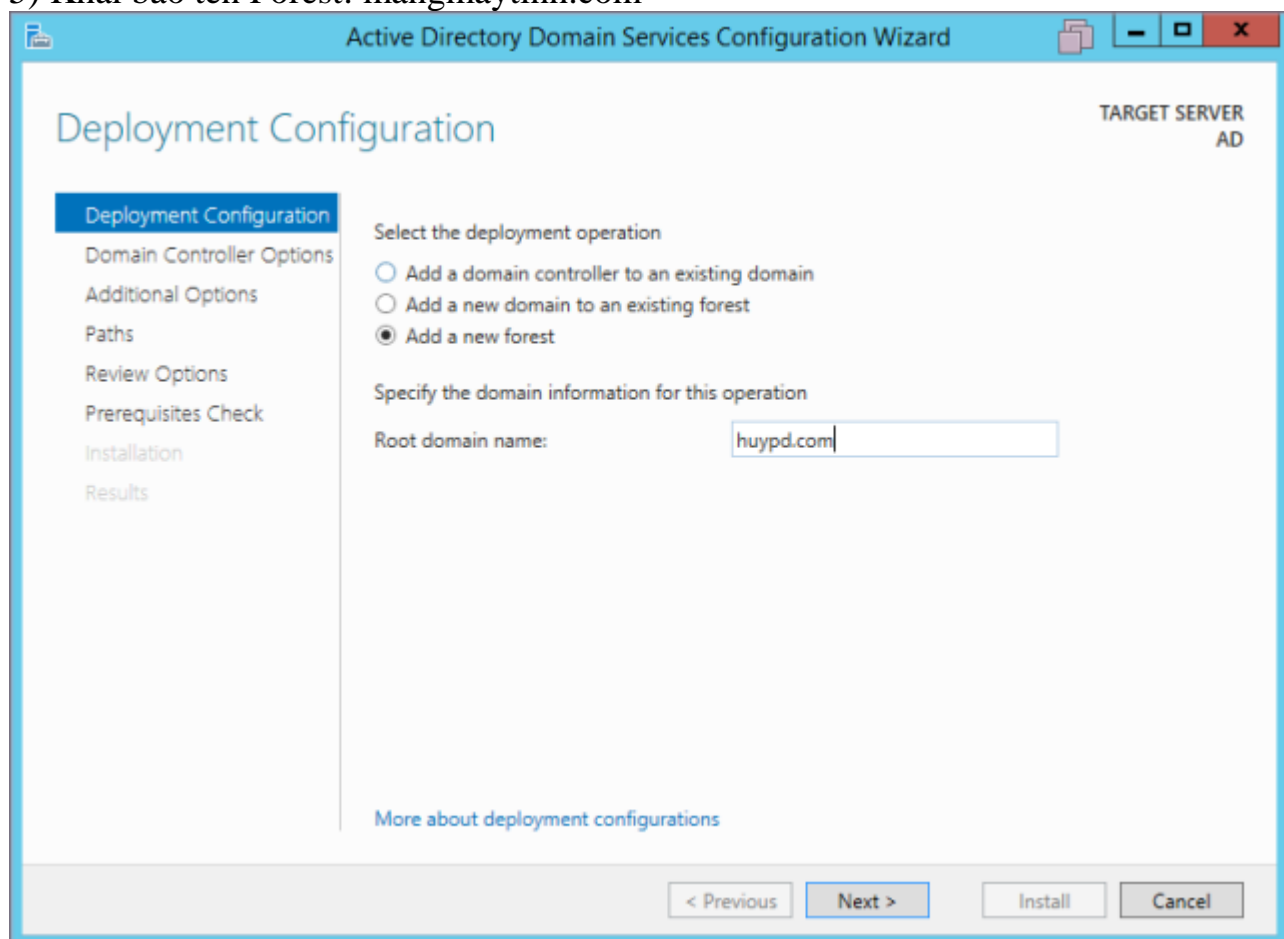




4) Sau khi đã cài xong, chọn “Promote this server to a domain controller” để khai báo thông tin AD



5) Khai báo tên Forest: mangmaytinhh.com



6) Đặt password cho Enterprise Admin và chọn cấp độ schema cho Forest functional level và Domain Functional Level

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the text 'Active Directory Domain Services Configuration Wizard' and standard window controls. The main window has a blue header with the title 'Domain Controller Options' and a 'TARGET SERVER AD' label in the top right corner. On the left is a navigation pane with the following items: 'Deployment Configuration', 'Domain Controller Options' (highlighted in blue), 'DNS Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select functional level of the new forest and root domain'. It contains two dropdown menus: 'Forest functional level:' and 'Domain functional level:', both set to 'Windows Server 2012 R2'. Below these is a section titled 'Specify domain controller capabilities' with three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). Further down is a section titled 'Type the Directory Services Restore Mode (DSRM) password' with two password fields labeled 'Password:' and 'Confirm password:', both containing masked characters. At the bottom of the main content area is a link that says 'More about domain controller options'. The bottom of the window features a navigation bar with four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER AD

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level: Windows Server 2012 R2

Specify domain controller capabilities

☒ Domain Name System (DNS) server
☒ Global Catalog (GC)
☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel

Active Directory Domain Services Configuration Wizard

Paths

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Specify the location of the AD DS database, log files, and SYSVOL

Database folder:

C:\Windows\NTDS

...

Log files folder:

C:\Windows\NTDS

...

SYSVOL folder:

C:\Windows\SYSVOL

...

TARGET SERVER

AD

More about Active Directory paths

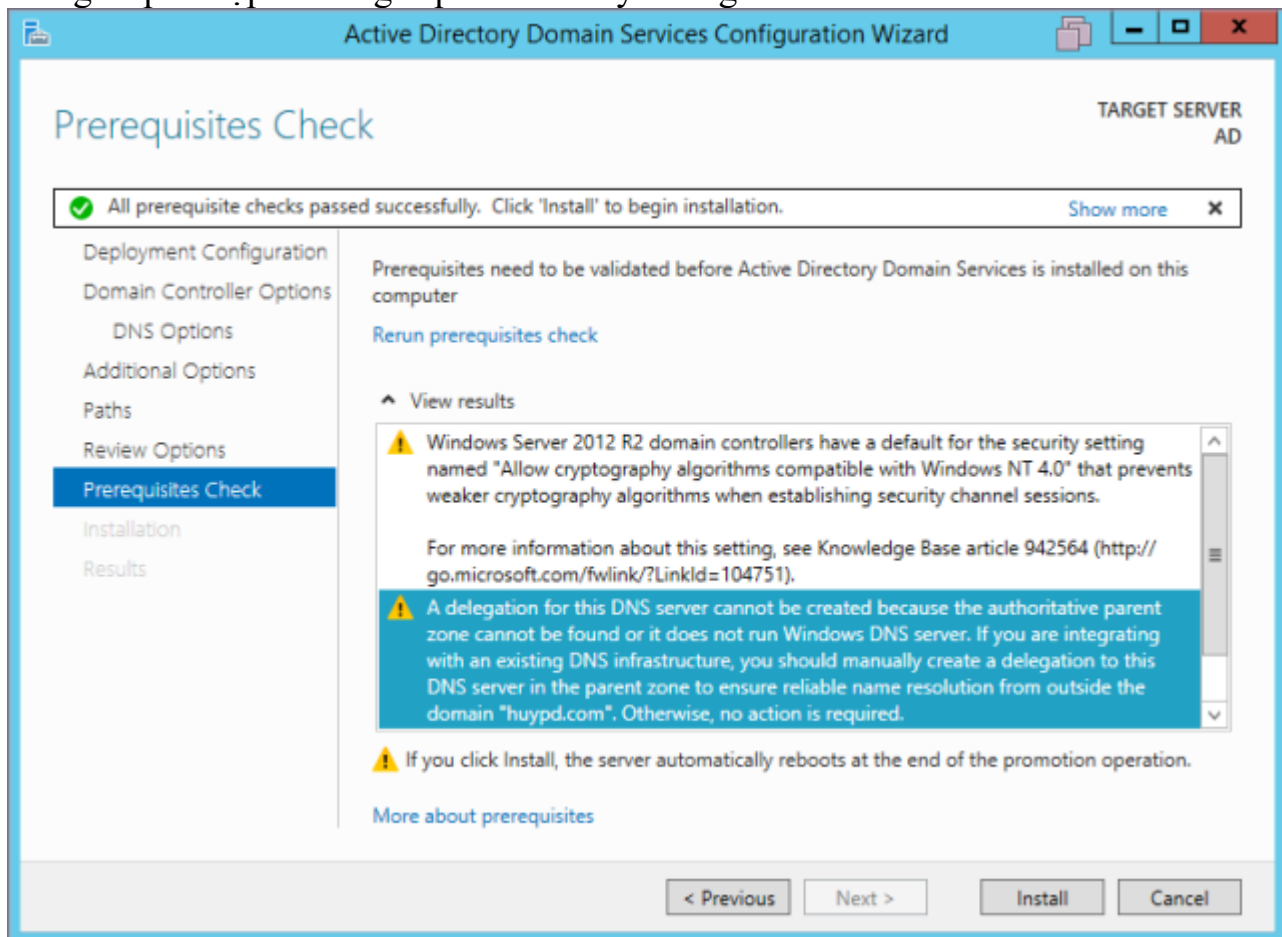
< Previous

Next >

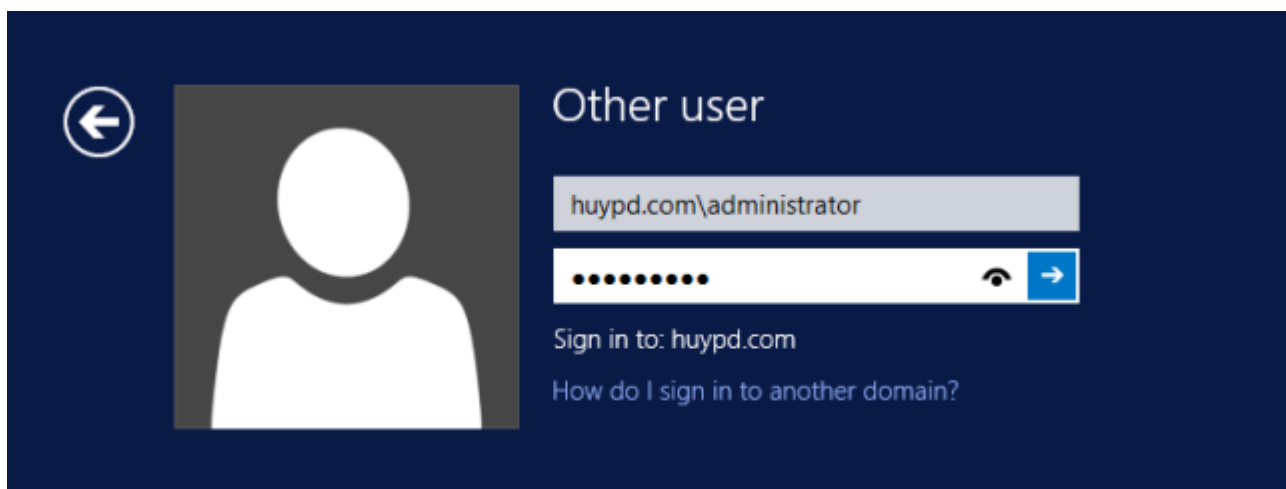
Install

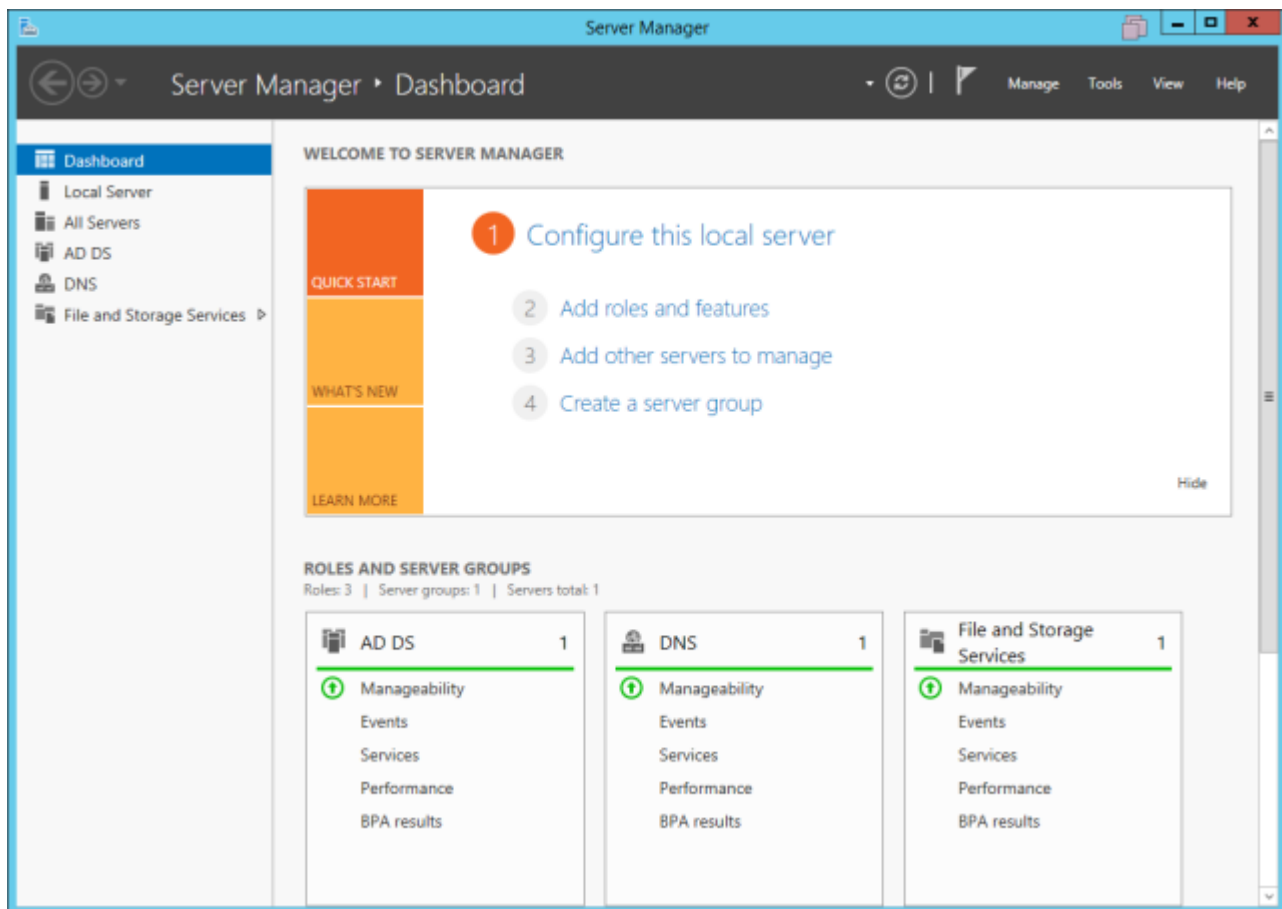
Cancel

7) Hệ thống sẽ tiến hành kiểm tra một cách chi tiết và an toàn, xem có đầy đủ thông số phù hợp để nâng cấp lên AD hay không.



8) Sau khi nâng cấp thì hệ thống sẽ restart lại và lúc này chúng ta dùng tài khoản Enterprise Administrator để logon vào máy.





3. Tạo Users, OU và phân quyền quản lý OU trên Windows Server 2012

Local User(s): là user(s) chỉ tồn tại trên chính máy client đó, user(s) đó chỉ có thể đăng nhập (logon) trên chính máy tính đó và sẽ không thể đăng nhập vào máy tính khác với user(s) đó.

Domain user(s) là user(s) được tạo trên AD của máy tính đóng vai trò là 01 Domain Controller, domain user(s) có thể đăng nhập vào bất kì máy tính trong hệ thống mạng (với điều kiện, máy tính đó được join vào domain)

Local Group: Cũng tương tự như local user, local group chỉ tồn tại trên máy tính đó, và để dễ quản lý, local group sẽ chứa những local user cùng nhóm (group) với mình

Vd: NhanSu_Group; KeToan_Group; KinhDoanh_Group; ...

Domain Group: Cũng tương tự như Domain user(s), domain group(s) tồn tại trên AD máy DC và chứa các domain user(s) tương ứng để giúp cho người quản trị hệ thống dễ quản lý

Organizational Unit (đơn vị tổ chức) : đại diện cho một tổ chức đơn lẻ mà trong đó chứa nhiều đơn vị (phòng ban) trong tổ chức đó, hoặc được sử dụng để phân biệt giữa thành phần nào đó cùng tên nhưng khác đơn vị tổ chức (OU). Ví dụ : user vietcuong trong OU IT và user VietCuong trong OU Instructor

- Một OU có thể chứa 01 hay nhiều OU khác, có thể chứa các domain groups và domain users

- Mục đích tạo một hay nhiều OU để sau này giúp cho người quản trị dễ dàng hơn trong việc quản lý, dễ triển khai công việc đến các domain user. Ví dụ : Deploy softwares (cài đặt từ xa và thực thi 01 cách tự động), tạo network drive, áp các chính sách của hệ thống (policies) cho các domain user(s)...

- Sau khi xây dựng thành công máy chủ Domain Controller trên Windows Server 2012 và tiến hành join các máy clients vào Domain, tiến hành tạo user, OU và phân quyền quản lý OU (Organizational Unit).

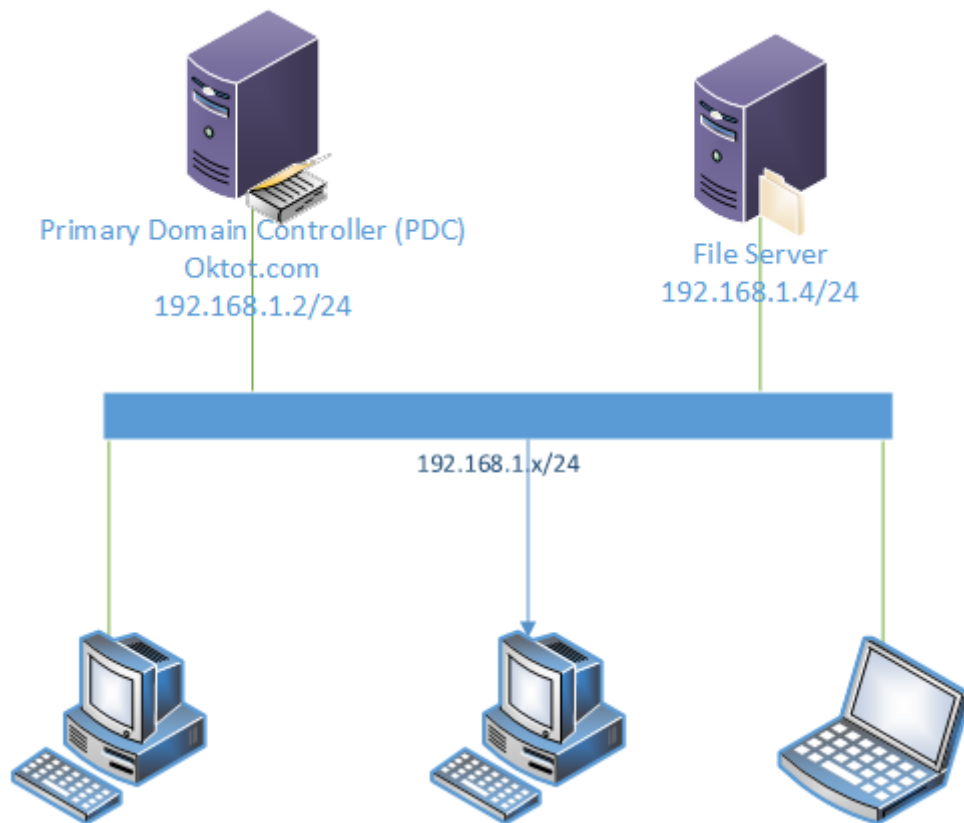
Tạo các OU quản lý theo các phòng ban: **P Lập Trình, P Điều Hành, P Quản Trị Mạng, Ban giám đốc, P Hành chính, P Kế toán, P Kinh doanh, P Thiết kế**. Sau đó Tạo các tài khoản người dùng theo OU tương ứng với phòng ban:

- **Ban giám đốc:** Nguyễn Văn Tâm, Trần Văn Phú
- **P Hành chính:** Nguyễn Đức Hoàng, Nguyễn Xuân Sang
- **P Kế toán:** Trần Thái Hà, Lê Minh Hoàng
- **P Kinh doanh:** Vũ Huy Hoàng, Nguyễn Thị Diệu, Nguyễn Đức Hùng
- **P Thiết kế:** Trần Thanh Bình, Nguyễn Thị Phụng Anh, Đặng Thanh Tùng, Nguyễn Phi Thái, Trần Thành Nam, Võ Thị Tuyết, Trần Thanh Thủy, Lê Hải Sơn.
- **Các User gạch chân là user quản lý OU.**

a. Chuẩn bị

- 01 máy Windows Server 2012 đã triển khai làm **Primary Domain Controller (PDC)**
- 01 máy Domain member chạy Windows 7/8/10.

Mô hình hệ thống (Forest: mangmaytinhh.com)



b. Các bước chính

Bước 1. Mở công cụ Active Directory Users and Computers

Bước 2. Tạo các OU và User

Bước 3. Ủy quyền cho các User quản lý OU

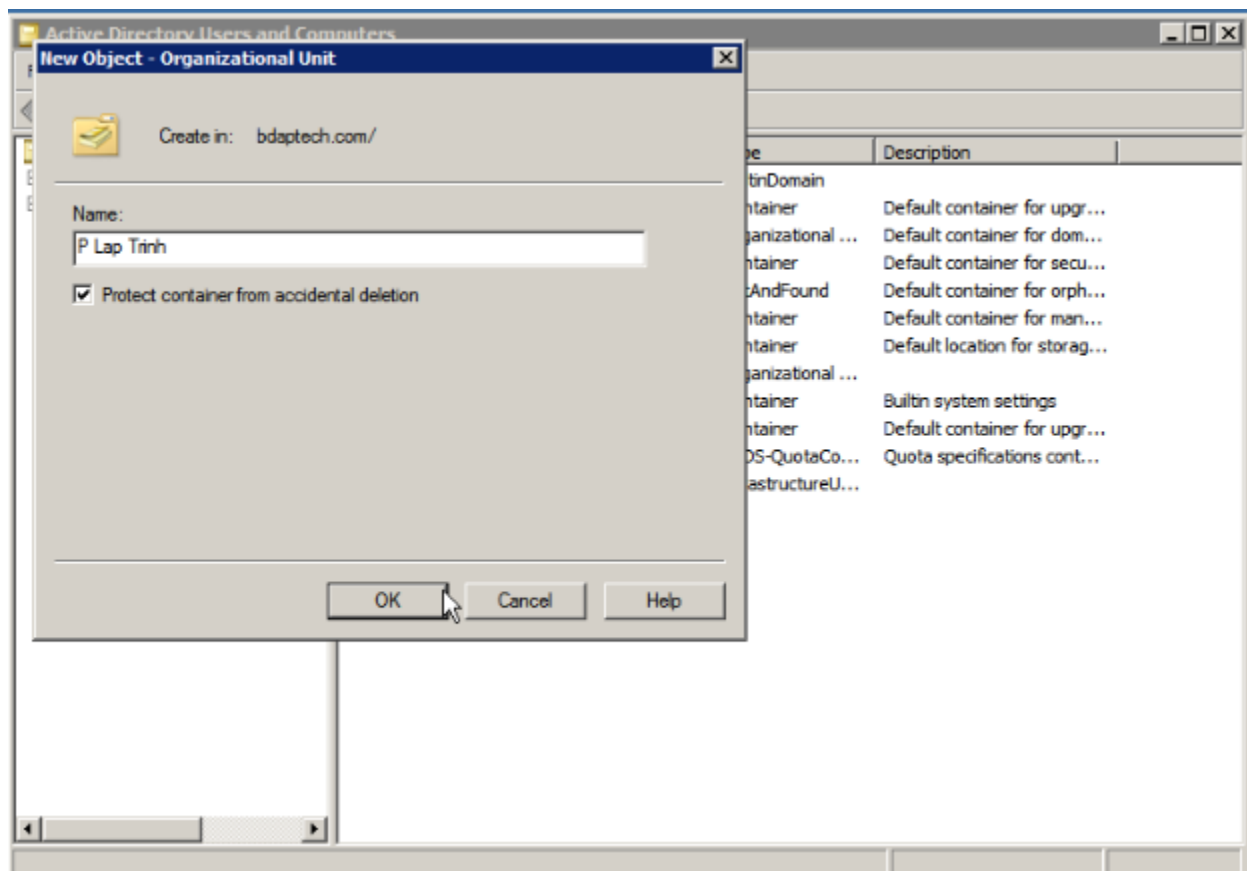
Bước 4. Đăng nhập với quyền User quản lý để kiểm tra

Tạo tài khoản người dùng và tài khoản nhóm trên miền **mangmaytinhh.com**. Thiết lập thuộc tính cho các đối tượng người dùng và nhóm như sau:

- Tất cả các tài khoản người dùng trên là thành viên nhóm Backup Operator
- Tài khoản người dùng manhnv và tottd phải thay đổi mật khẩu khi đăng nhập vào hệ thống lần đầu tiên
- Người dùng tungnv không được phép đổi mật khẩu từ máy trạm.
- Tạm khóa tài khoản người dùng tungnv vì anh này đi học nước ngoài.
- Nhân viên thuộc nhóm **Kinh doanh** chỉ được phép đăng nhập vào mạng từ 7h sáng đến 9h tối mỗi ngày, từ thứ 2 đến thứ 6
- Sử dụng công cụ Active Directory Users and Computers để tạo và quản lý tài khoản người dùng.

Tạo OU:

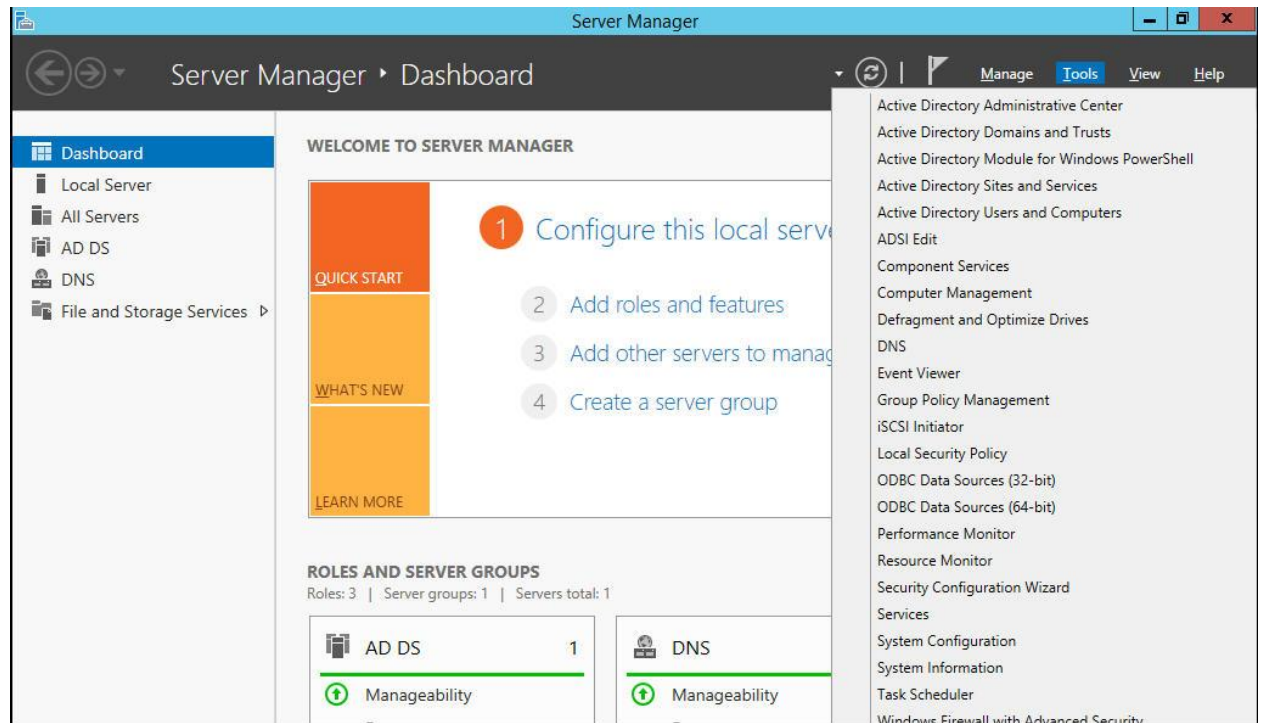
- **Start > Programs > Administrative Tools > Active Directory Users and Computer.**
- Nhấp phải trên domain **mangmaytinh.com** > **New > Organizational Unit.**
- Nhập vào OU cần tạo.

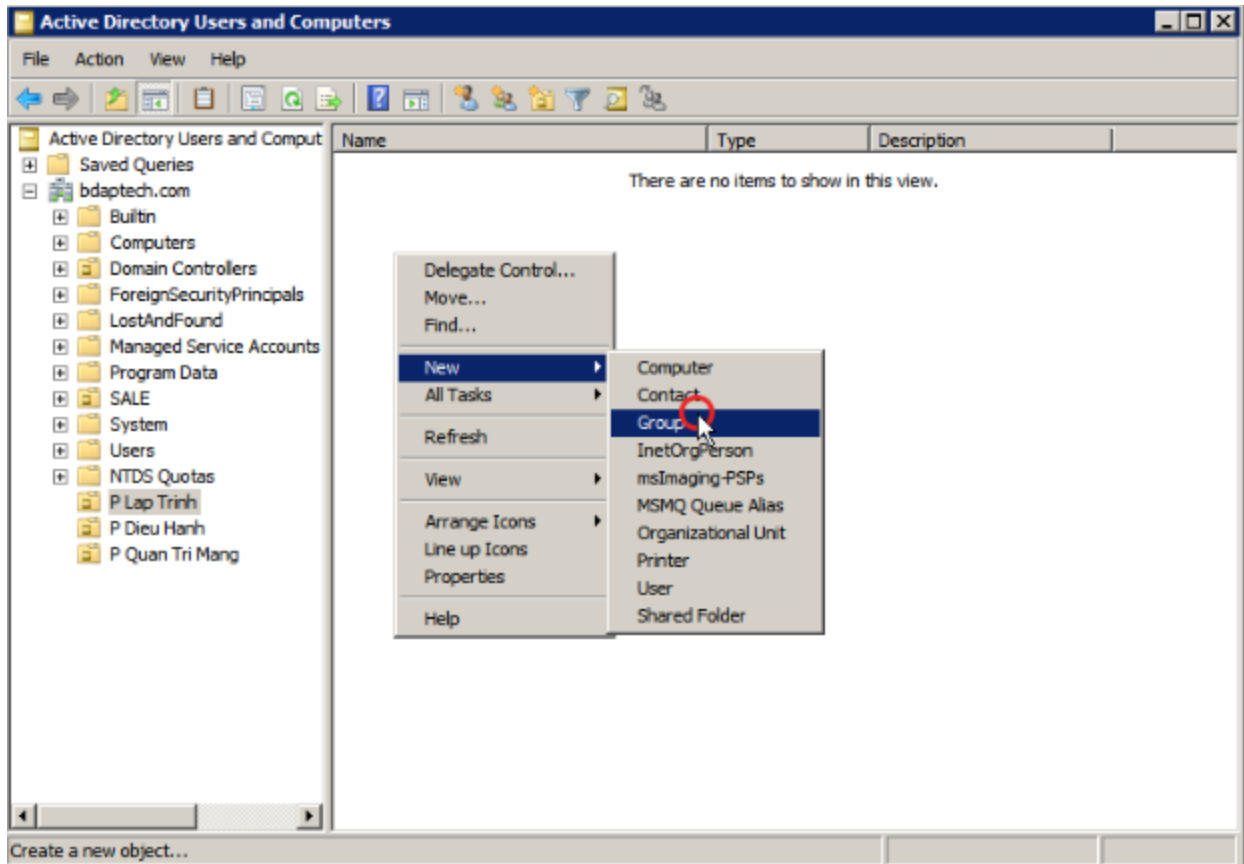


- Tương tự tạo các **OU** của phòng ban: **P Lập Trình, P Quản Trị Mạng, P Điều Hành.**

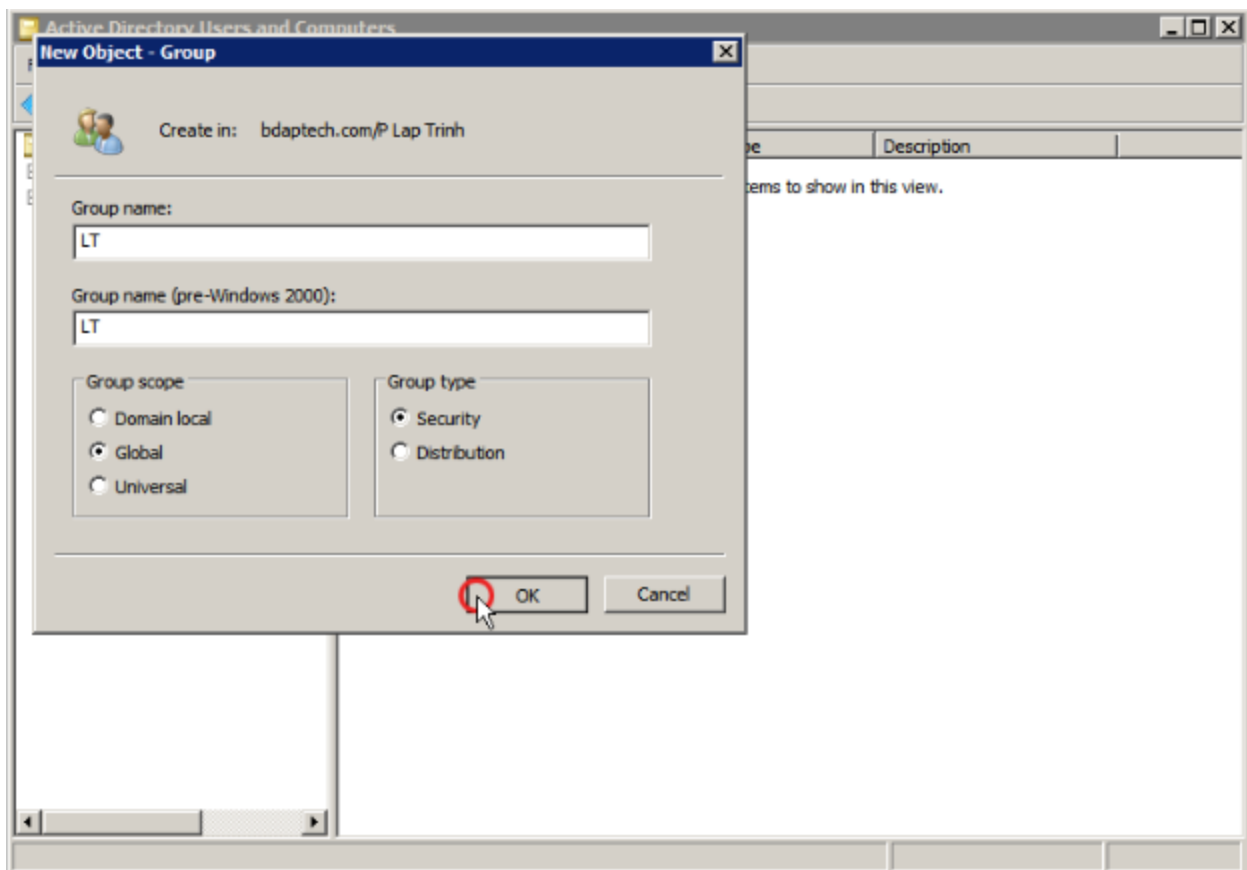
Tạo tài khoản nhóm và tài khoản người dùng:

- **Server Manager > Tools > Active Directory Users and Computers.**
Nhấp phải chuột trên mục **Users > New > Group**.

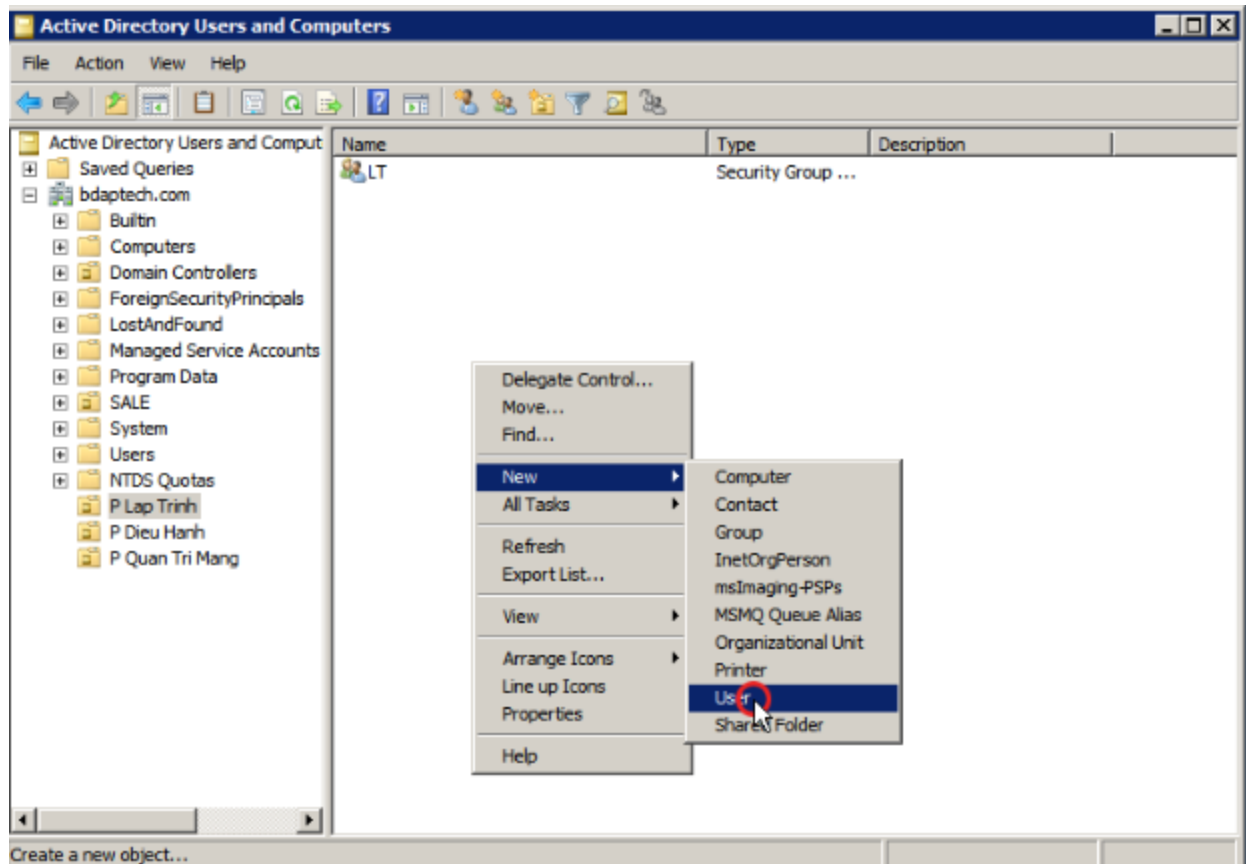




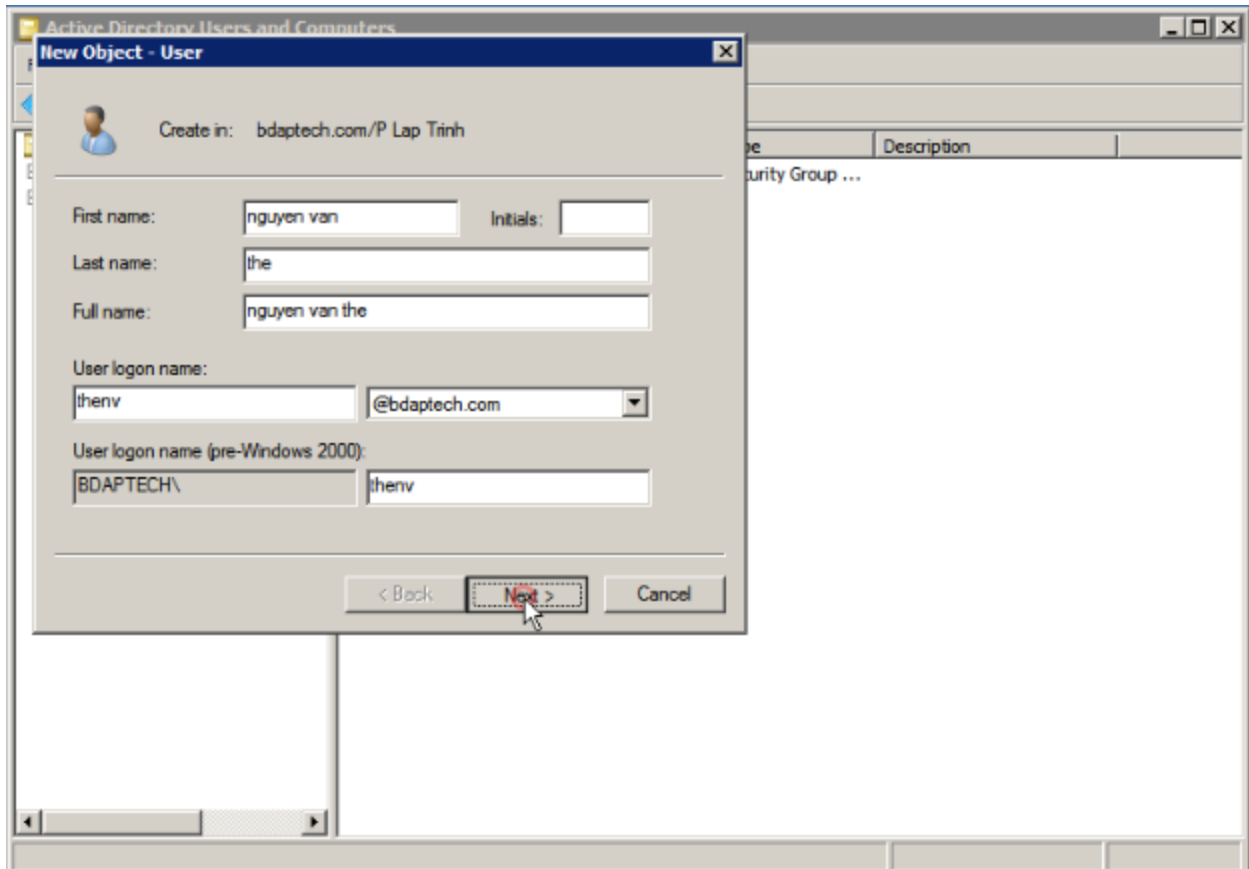
- Tại cửa sổ **New Object – Group** nhập tên nhóm cần tạo và nhấn **OK** để kết thúc.



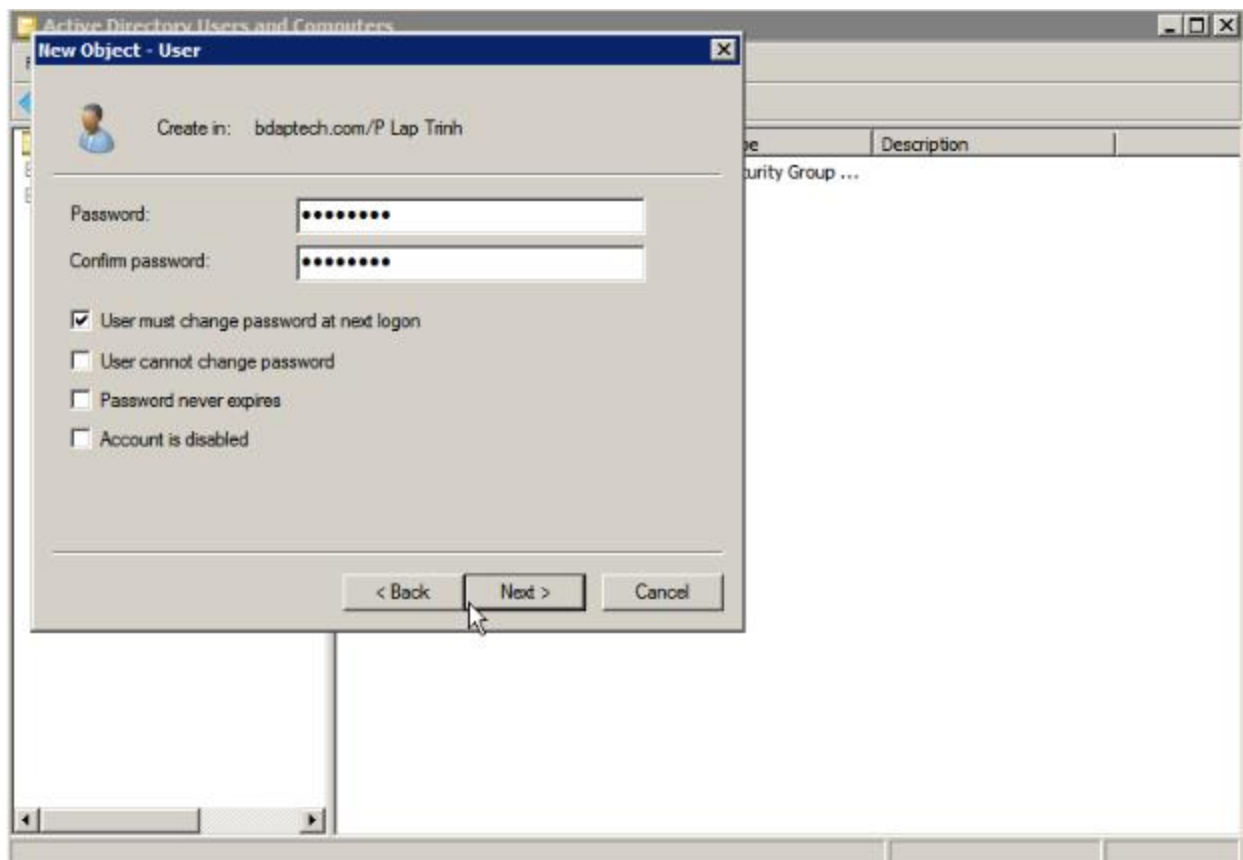
- Tương tự tạo tài khoản nhóm khác
- **Tạo tài khoản người dùng:** Nhấp phải trên thư mục **User > New > User**.



- Hộp thoại tạo tài khoản người dùng xuất hiện, nhập thông tin và nhấn **Next**



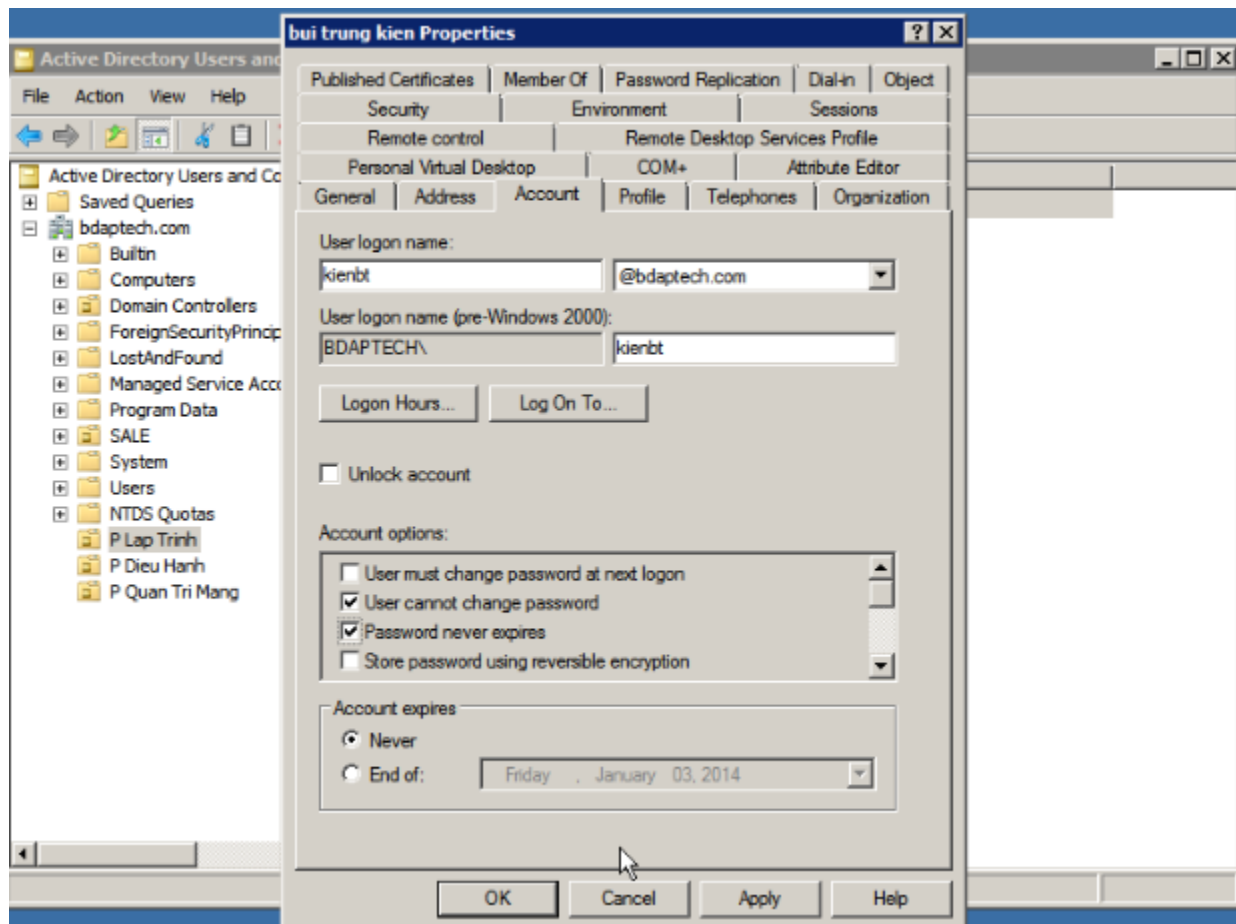
- Tại hộp thoại kế tiếp, nhập thông tin về mật khẩu, nhấn Next. (với tùy chọn **User must change password at next logon** thì người dùng sẽ phải thay đổi mật khẩu khi đăng nhập vào hệ thống lần kế tiếp).
- Tại hộp thoại tiếp theo, nhấn **Finish** để hoàn tất việc tạo tài khoản người dùng.



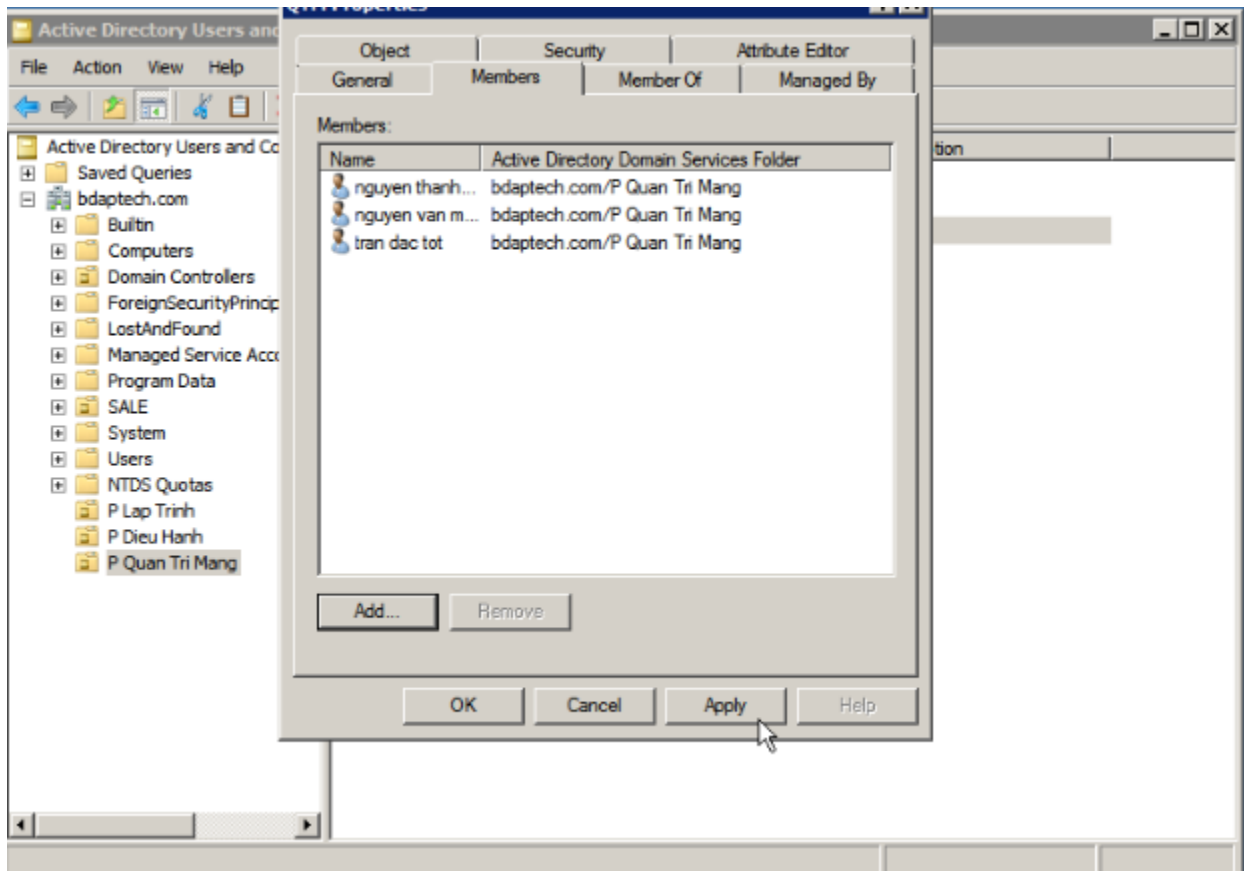
Tương tự cho các user khác.

Thay đổi thuộc tính tài khoản:

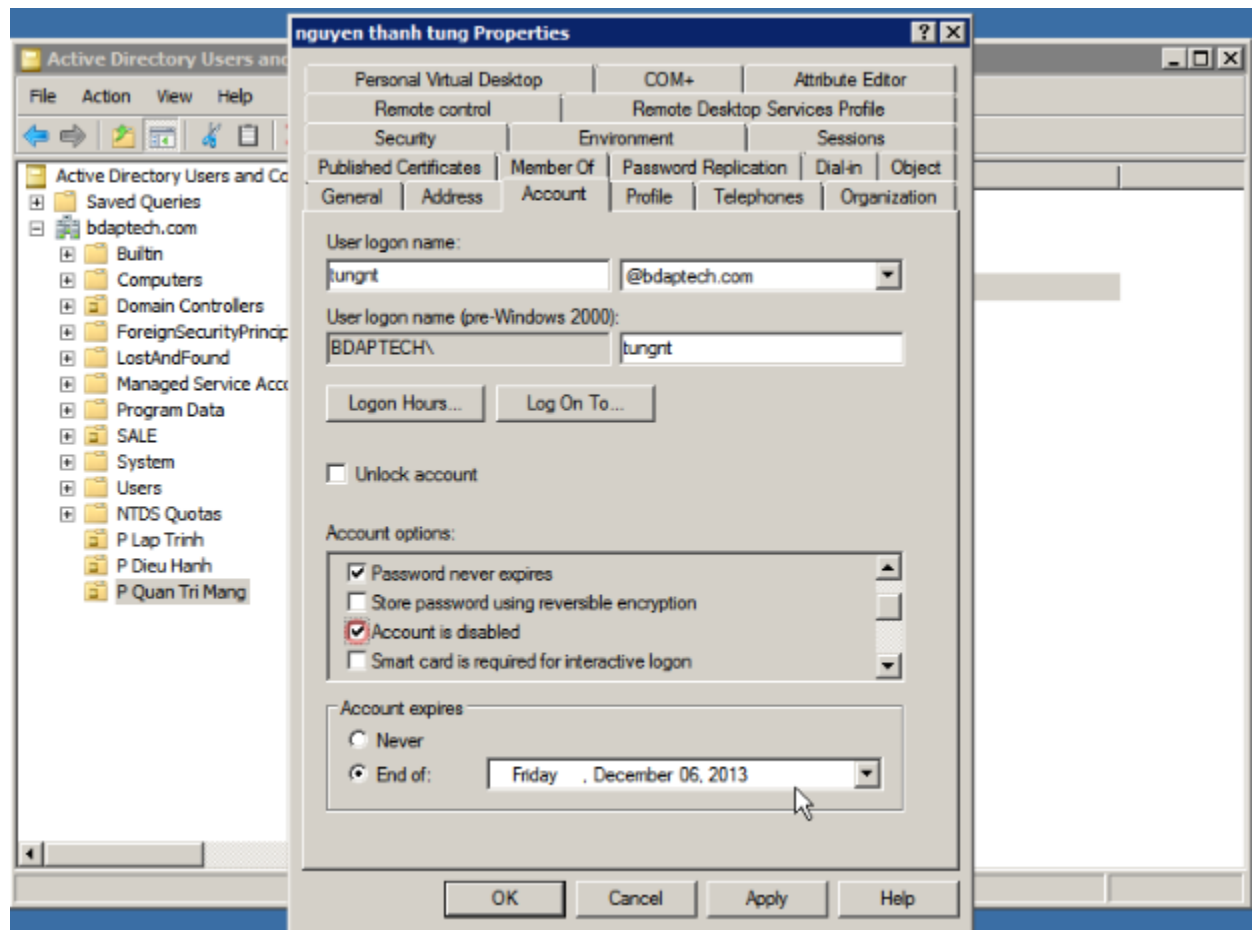
- **Start > Programs > Administrative Tools > Active Directory User and Computers > chọn miền mangmaytinh.com > Users**
- Phải chuột lên tài khoản người dùng cần thay đổi thông tin, chọn **Properties**, chọn tab **Account**.



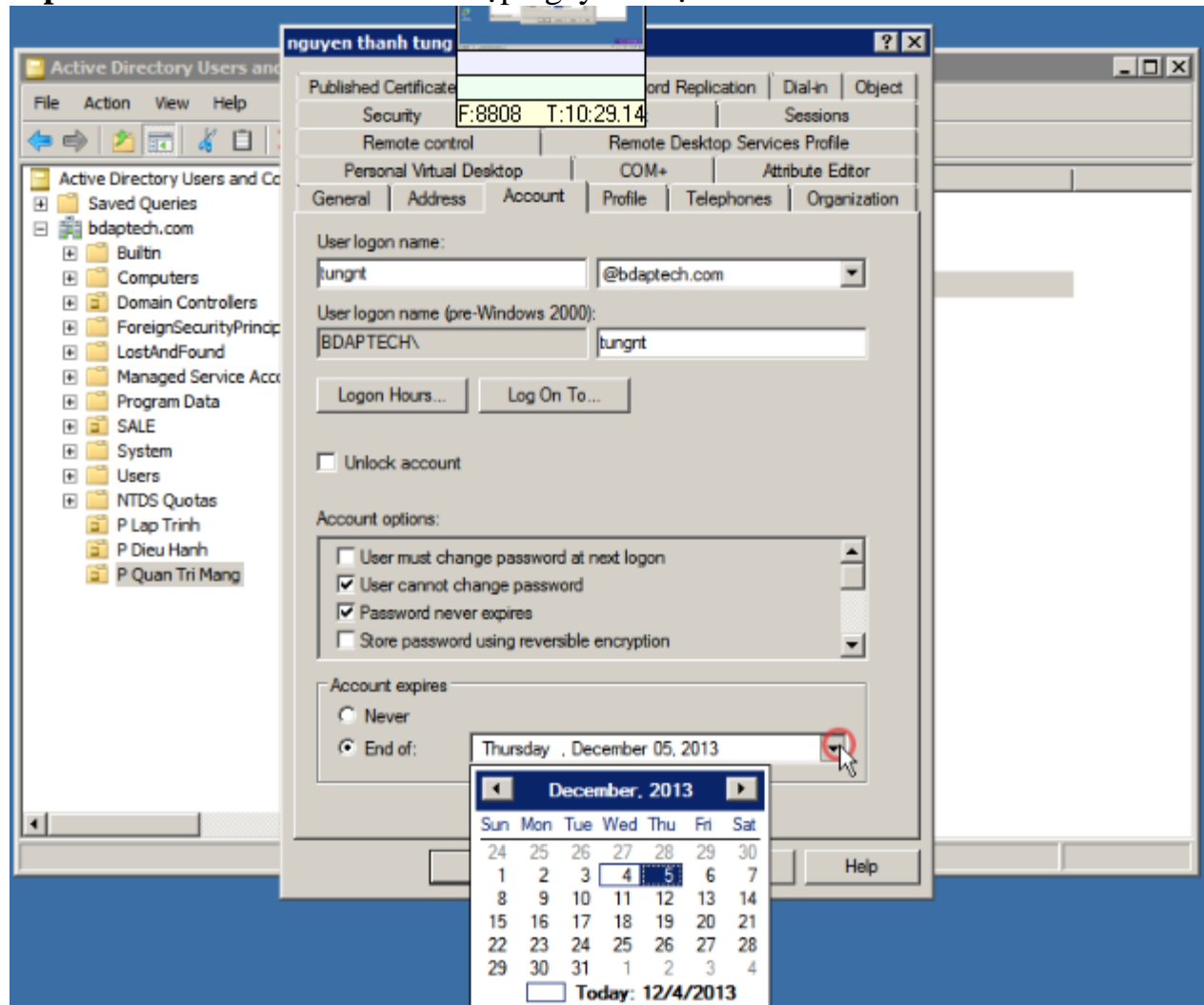
Để thêm tài khoản thenv vào nhóm **QuanTriMang** và nhóm **Backup Operators** chọn tab **Member of** và chọn **Add** để thêm thông tin nhóm người dùng cho tài khoản:



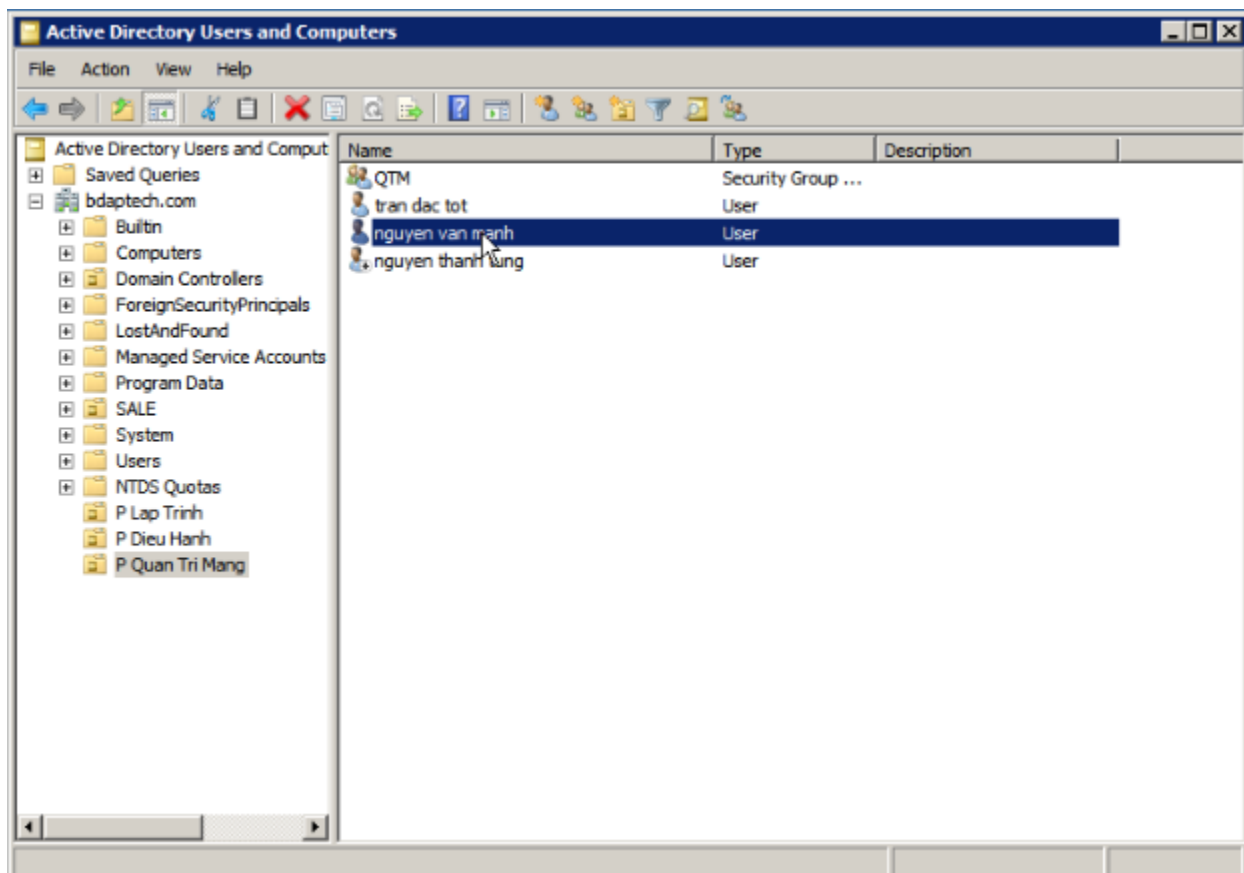
- Tương tự, thực hiện tạo tài khoản cho tài khoản anhln, hungtn và gia nhập vào nhóm cho các User này tùy theo yêu cầu.
- Trên tài khoản **hungtn**, để thiết lập không cho phép thay đổi mật khẩu và khóa tài khoản, trên tab **Account** của tài khoản **hungtn** tick vào **User cannot change password** và **Account is disabled**.



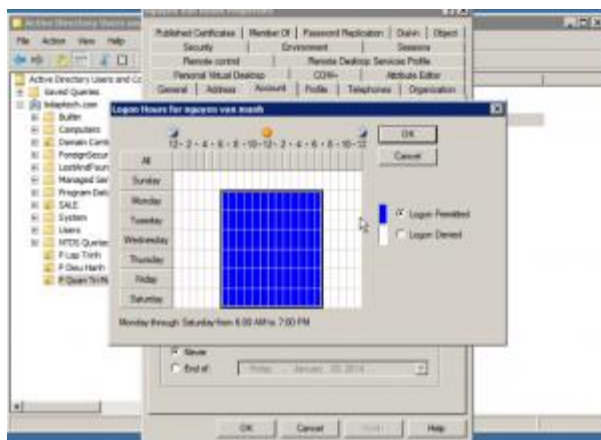
- Để thiết lập hạn sử dụng cho tài khoản **hungtn**, trong phần **Account expires** tick vào **End of** và thiết lập ngày hết hạn của tài khoản



- Để thiết lập thời gian đăng nhập cho người dùng thuộc nhóm Lập Trình, click chọn các thành viên thuộc nhóm Lập Trình, nhấn phải chọn **Properties**



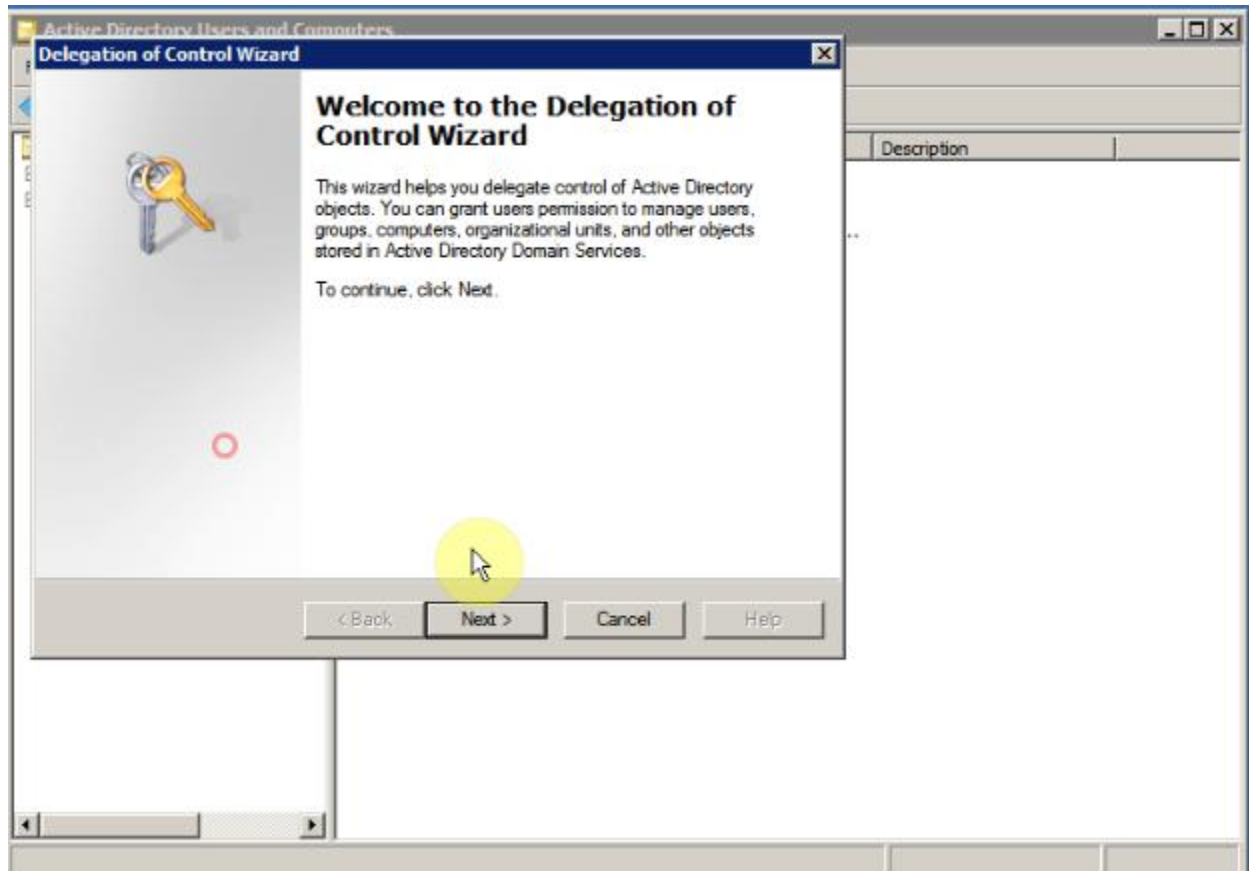
Tại tab **Account** tick chọn **Logon hours** rồi nhấp vào **Logon hours** để tiếp tục



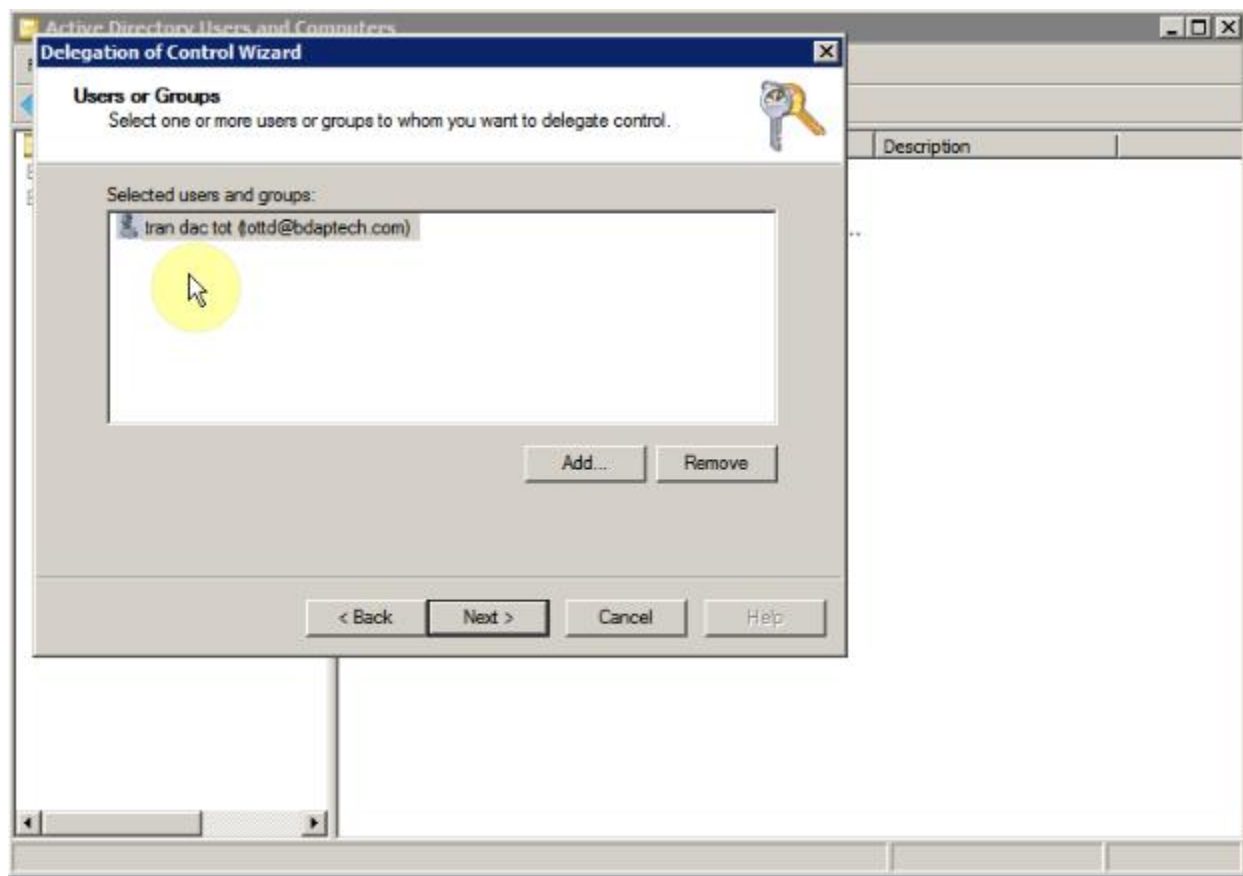
- Sau khi thiết lập thời gian đăng nhập, nhấn **OK** để kết thúc.

Thiết lập tài khoản có quyền quản trị trên OU:

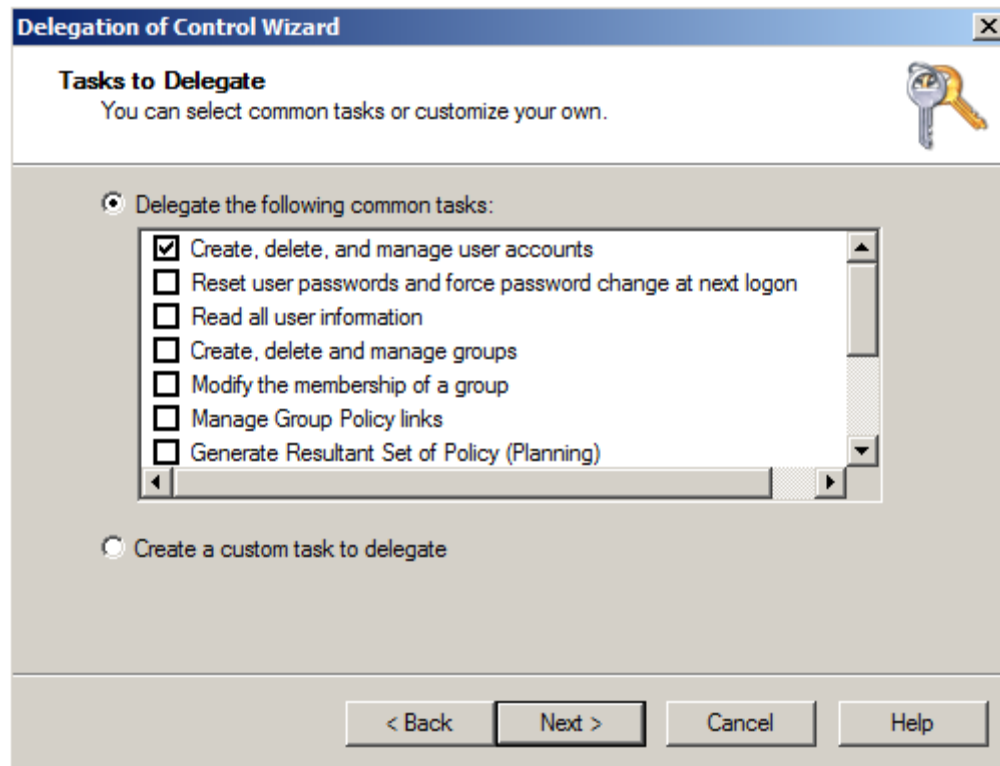
- Nhấp phải trên **OU** cần thiết lập > **Delegate control**, màn hình **Welcome to the Delegation of Control Wizard** xuất hiện, nhấp **Next**.



- Tại màn hình **User or Groups**, nhấp **Add** để thêm vào đối tượng cần thiết lập quyền hạn, nhấn **Next**.



- Tại màn hình **Task to Delegete**, chọn các tác vụ người quản trị được phép thực hiện trên đối tượng OU, sao khi thiết lập xong > nhấn **Next**.



- Tại màn hình **Completing the Delegation of Control Wizard**, nhấn **Finish** để hoàn tất.